

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001 年 5 月 25 日 (25.05.2001)

PCT

(10) 国際公開番号
WO 01/37479 A1

- (51) 国際特許分類: H04L 9/08
- (21) 国際出願番号: PCT/JP00/08107
- (22) 国際出願日: 2000 年 11 月 16 日 (16.11.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願平 11/327011
1999 年 11 月 17 日 (17.11.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 Kanagawa

(JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目 14 番 14 号 Tokyo (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目 6 番地 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通 2 丁目 5 番 5 号 Osaka (JP).

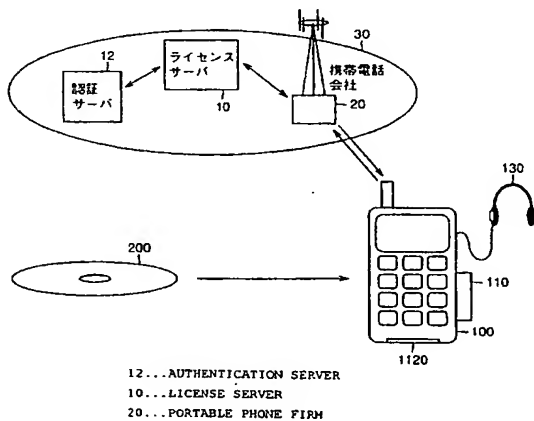
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 畑中正行 (HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目 14 番 14 号 日本コロムビア株式会社

[続葉有]

(54) Title: DATA DISTRIBUTING SYSTEM AND RECORDING MEDIUM USED FOR IT

(54) 発明の名称: データ配信システムおよびそれに用いる記録媒体



(57) Abstract: Encrypted music data and additional information necessary for accessing a server (30) are copied from a CD-ROM (200) onto a memory card (110). The memory card (110) receives via a digital portable phone network the distribution of a contents decoding key (Kc) necessary for decoding encrypted music data and control information data (AC1) for limiting the number of accesses to the memory card from the server (30).

(57) 要約:

CD-ROM (200) からメモリカード (110) へは、暗号化された音楽データと、サーバ (30) へアクセスするために必要な付加情報が複製される。メモリカード (110) は、デジタル携帯電話網を介して、サーバ (30) から暗号化音楽データを復号処理するために必要なコンテンツ復号キー (Kc) やメモリカードへのアクセス回数を制限するための制御情報データ (AC1) 等の配信を受ける。

WO 01/37479 A1



内 Tokyo (JP). 利根川 忠明 (TONEGAWA, Tadaaki) [JP/JP]. 中田 順二 (NAKATA, Junji) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL,

PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

データ配信システムおよびそれに用いる記録媒体

5 技術分野

本発明は、携帯電話等の端末に対してコンテンツ情報を供給し、かつこのコンテンツ情報を再生可能とするための情報を配送するためのデータ配信システムに関するものである。

10 背景技術

インターネットや情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15 このような情報通信においてはデジタル信号により情報が伝送される。したがって、例えば、上述のような情報通信網において伝送された音楽や映像情報を各ユーザが、音質や画質の劣化をほとんど生じさせることなくコピーを行なうことが可能である。言いかえると、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のため
20 ある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の利用に際して、適切な料金を徴収することが可能な著作権者にとっても、かえって不利益となる。

25 ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を再生可能な状態で記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽情報のコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル

録音等を行う個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、ユーザは、CDからMDへのコピーは許されるが、MDからMDへのコピーはできない。

- 5 そのような事情からも、音楽情報や画像情報等のコンテンツデータをデジタル情報として公衆に配布することに対しては、著作権保護のための十分な方策が講じられる必要がある。

- 10 例えば、著作権者の側で、新曲のプロモーションなどのために音楽データを、何らかの配布手段を介して不特定多数のユーザに配布したい場合がある。しかしながら、この場合に、単純に上記デジタル情報通信網を介して再生可能な音楽データを無条件に配信してしまうと、著作権者が料金をユーザから回収することが困難になってしまう。

- 15 さらに、ユーザが上記のような音楽データの供給を受けた場合でも、一度供給された音楽データが、さらに再生可能な状態で無制限に複製されることを防止することも必要となる。

- 20 一方で、音楽データの配信システムとして、駅頭やコンビニエンスストアなどに設置することを目的とした、音楽データ販売用の自動販売機の運用実験等も開始されている。この場合は、音楽データは、上記デジタル情報通信網を介して自動販売機に配信され、ユーザは当該音楽コンテンツ情報をこの自動販売機から購入することになる。

- 25 しかしながら、このような自動販売機では、音楽データを、書込み可能な記録媒体、例えば、MDへ記録することにより、音楽データの販売を行なうこととしている。この場合、例えば、一曲あたりの録音時間が数十秒であるとする、10曲程度まとめて購入しようとするユーザは、その購入のために数分以上待つことが必要になってしまう。

発明の開示

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、例えば携帯電話等の情報通信網を介してデータの授受を行

なうことが可能なユーザに対して、著作権を保護しつつ、音楽コンテンツデータの供給を行なうことが可能なデータ配信システムを提供することである。

5 この発明の他の目的は、情報通信網、例えば携帯電話等の情報通信網を介してデータの授受を行なうことが可能なユーザに対して、著作権を保護しつつ、音楽コンテンツデータの供給を行なうことが可能な記録媒体を提供することである。

この発明のさらに他の目的は、配信されたコンテンツデータが、著作権者の許可なく無制限に再生されたり複製されることを防止することが可能なデータ配信システムを提供することである。

10 係る目的を達成するために本願発明に係るデータ配信システムは、暗号化コンテンツデータを複数のユーザの各端末に配布するためのデータ配信システムであって、記録媒体と、配信サーバと、コンテンツデータ再生装置とを備える。記録媒体は、暗号化コンテンツデータと、暗号化コンテンツデータの復号処理に使用する復号情報データを取得するための平文付加情報データとを記録する。配信サーバは、復号情報データを情報伝達網を介して配信する。コンテンツデータ再生装置は、記録媒体から暗号化コンテンツデータおよび平文付加情報データを受けて格納し、平文付加情報データに基づいて特定される配信サーバから情報伝達網を介して復号情報データを受信して、暗号化コンテンツデータを復号情報データに応じて復号し、暗号化コンテンツデータを復号して得られるコンテンツデータに対応する情報を出力する。

20 好ましくは、コンテンツデータ再生装置は、読取り装置と、メモリと、受信装置と、復号装置と、再生装置とを含む。読取り装置は、記録媒体から暗号化コンテンツデータおよび平文付加情報データを読み取る。メモリは、読み取り装置から与えられた暗号化コンテンツデータおよび平文付加情報データを受けて格納する。受信装置は、情報伝達網を介して特定された配信サーバから復号情報データを受信する。復号装置は、暗号化コンテンツデータを復号情報データに基づいて平文化する。再生装置は、復号装置からの出力を受けて、コンテンツデータに対応する情報を再生する。

さらに好ましくは、メモリは、コンテンツデータ再生装置から着脱可能なメモリカードである。

あるいは、好ましくは、情報伝達網は、デジタル携帯電話網であって、コンテンツデータ再生装置は、携帯電話機を含む。携帯電話機は、データ入出力端子と、メモ리카ードと、復号装置と、再生装置とを含む。データ入出力端子は、外部との間でデジタルデータの授受が可能である。メモ리카ードは、携帯電話機に着脱可能であって、記録媒体から読み出されデータ入出力端子を介して与えられた暗号化コンテンツデータおよび平文付加情報データを受けて格納する。復号装置は、デジタル携帯電話網を介して特定された配信サーバから受信した復号情報データに基づいて、暗号化コンテンツデータを平文化する。再生装置は、復号装置からの出力を受けて、コンテンツデータに対応する情報を再生する。

10 あるいは、好ましくは、情報伝達網は、デジタル携帯電話網であって、コンテンツデータ再生装置は、デジタル携帯電話網を介して特定された配信サーバから復号情報データを受信するための携帯電話機を含む。携帯電話機は、復号装置と、再生装置とを有する。復号装置は、暗号化コンテンツデータを復号情報データに基づいて平文化する。再生装置は、復号装置からの出力を受けて、コンテンツデータに対応する情報を再生する。コンテンツデータ再生装置は、メモ리카ードと、メモ리카ードドライブ装置とをさらに含む。メモ리카ードは、携帯電話機に着脱可能であって、暗号化コンテンツデータおよび平文付加情報データを受けて格納する。メモ리카ードドライブ装置は、記録媒体からメモ리카ードへのデータ転送を行う。

20 あるいは、好ましくは、情報伝達網は、デジタル携帯電話網であって、コンテンツデータ再生装置は、デジタル携帯電話網を介して特定された配信サーバから復号情報データを受信するための携帯電話機を含む。携帯電話機は、復号装置と、再生装置とを有する。復号装置は、暗号化コンテンツデータを復号情報データに基づいて平文化する。再生装置は、復号装置からの出力を受けて、コンテンツデータに対応する情報を再生する。コンテンツデータ再生装置は、メモ리카ードと、メモ리카ードドライブ装置とをさらに含む。メモ리카ードは、携帯電話機に着脱可能であって、暗号化コンテンツデータおよび平文付加情報データを受けて格納する。メモ리카ードドライブ装置は、記録媒体からメモ리카ードへのデータ転送を行う。

記録媒体は、暗号化コンテンツデータ、平文付加情報、予め定められた複数の固有鍵を特定するための特定データおよび特定データに対応する固有鍵により復号可能な暗号化をされた復号情報データを記録している。メモ리카ードドライブ装置は、固有鍵保持部と、固有鍵復号処理部とを含む。固有鍵保持部は、特定データにより選択的に指定される複数の固有鍵を保持する。固有鍵復号処理部は、複数の固有鍵のうち、記録媒体からの特定データに対応する固有鍵で、記録媒体からの暗号化された復号情報データを復号して、復号情報データを受理する。少なくともメモ리카ードドライブ装置において復号情報データを受理可能であることに基づいて、メモ리카ードへ受理した復号情報データが転送される。

この発明の他の局面に従うと、暗号化コンテンツデータを複数のユーザの各端末に配布するためのデータ配信システムであって、記録媒体と、コンテンツデータ再生装置とを備える。記録媒体は、暗号化コンテンツデータと、暗号化コンテンツデータの復号処理に使用する復号情報データを取得するための平文付加情報データとを記録する。コンテンツデータ再生装置は、記録媒体から暗号化コンテンツデータおよび平文付加情報データを受けて格納し、平文付加情報データに基づいて特定される配信サーバから情報伝達網を介して復号情報データを受信して、暗号化コンテンツデータを復号情報データに応じて復号し、暗号化コンテンツデータを平文化して得られるコンテンツデータに対応する情報を出力する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータを複数のユーザの各端末に配布するために、暗号化コンテンツデータの復号処理に使用する復号情報データを情報伝達網を介して配信するための配信サーバを備え、各端末は、暗号化コンテンツデータおよび平文付加情報データを受けて格納し、平文付加情報に基づいて特定される配信サーバから情報伝達網を介して復号情報データを受信して、暗号化コンテンツデータを復号情報データに応じて復号し、暗号化コンテンツデータを復号して得られるコンテンツデータに対応する情報を出力するためのコンテンツデータ再生装置とを備えるデータ配信システムに用いられる記録媒体であって、第1の領域と、第2の領域とを備える。第1の領域は、少なくとも暗号化コンテンツデータを記録する。第2の領域は、暗号化コンテンツデータの復号処理に使用する復号情報データを取得するための平文付加情報データとを

記録する。

したがって、本願発明にかかる配信システムでは、携帯電話等の情報通信網を介してデータの授受を行なうことが可能なユーザに対して、著作権を保護しつつ、容易に音楽コンテンツデータの供給を行ない、かつ、ユーザは短時間で音楽の再生を行うことが可能となる。また、本発明にかかる記録媒体を用いても、携帯電話等の情報通信網を介してデータの授受を行なうことが可能なユーザに対して、著作権を保護しつつ、音楽コンテンツデータの供給を行ない、かつ、ユーザは短時間で音楽の再生を行うことが可能となる。しかも、配信された復号情報データは、著作権者の許可無く複製されることを防止することが可能となる。

10

図面の簡単な説明

図 1 は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図 2 は、図 1 に示したデータ配信システムにおいて使用される通信のためのキーデータ（鍵データ）やライセンス情報データ等の特性をまとめて説明するための図である。

図 3 は、図 1 に示したライセンスサーバ 10 の構成を示す概略ブロック図である。

図 4 は、図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

図 5 は、図 4 に示したメモリカード 110 の構成を説明するための概略ブロック図である。

図 6 は、データ配信システムにおける CD-ROM 200 からのデータ複製動作を説明するためのフローチャートである。

図 7 は、ライセンス情報データ等を携帯電話網を介して携帯電話機 100 に配信する動作を説明するための第 1 のフローチャートである。

図 8 は、ライセンス情報データ等を携帯電話網を介して携帯電話機 100 に対して配信する動作を説明するための第 2 のフローチャートである。

図 9 は、携帯電話機 100 内において、音楽情報を復号化し、音楽として外部

に出力するための再生処理を説明するフローチャートである。

図 10 は、本発明の実施例 2 のデータ配信システムの構成を示す概念図である。

図 11 は、図 10 に示したメモ리카ードドライブ装置 500 の構成を示す概略ブロック図である。

5 図 12 は、CD-ROM 200 からメモ리카ード 110 へ暗号化音楽データを複製する動作を説明するための第 1 のフローチャートである。

図 13 は、CD-ROM 200 からメモ리카ード 110 へ暗号化音楽データを複製する動作を説明するための第 2 のフローチャートである。

10 図 14 は、実施例 3 のデータ配信システムにおいて使用される通信のためのキーデータ（鍵データ）やライセンス情報データ等の特性をまとめて説明するための図である。

図 15 は、実施例 3 のライセンスサーバ 31 の構成を示す概略ブロック図である。

図 16 は、実施例 3 の携帯電話機 101 の構成を示す概略ブロック図である。

15 図 17 は、ライセンス情報データ等を携帯電話網を介して携帯電話機 101 に配信する動作を説明するための第 1 のフローチャートである。

図 18 は、ライセンス情報データ等を携帯電話網を介して携帯電話機 101 に配信する動作を説明するための第 2 のフローチャートである。

20 図 19 は、携帯電話機 101 内において、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

発明を実施するための最良の形態

〔実施例 1〕

〔システムの全体構成〕

25 図 1 は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作権が存在するコンテン

ッデータ、例えば画像情報等を、他の情報通信網を介して配信する場合にも適用することが可能なものである。

5 また、データ再生装置として、データ再生機能を組み込んだ携帯電話機を例にとって説明するが以下の説明で明らかとなるように、本発明は携帯電話機に限定されることなく、音楽データを再生するために必要な情報データを入手するため情報通信網に接続可能なデータ再生装置であれば適用することが可能である。

図1を参照して、携帯電話機100を利用するユーザ1には、暗号化された音楽データを第1の記憶領域に記録し、かつ当該音楽データに関する著作権や後に説明するサーバへのアクセス条件等の平文の付加情報データを第2の記憶領域に
10 記録した記録媒体、例えば、CD-ROM (Compact Disc Read Only Memory) 200が配布される。このCD-ROM 200上の音楽データは上述のとおり暗号化されているため、携帯電話ユーザ1は、そのままの状態では、音楽データを再生することができない。

携帯電話ユーザ1の携帯電話機100は、例えば、CD-ROM 200に記録された暗号化音楽データおよび平文付加情報データを読み出すパーソナルコンピュータ（図示せず）から、これらのデータを受取るためのコネクタ1120を備えている。携帯電話機100は、上記暗号化音楽データおよび平文付加情報データを記録し、かつ、音楽データに対して行われた暗号化について復号処理を行って携帯電話機100中の音楽再生部（図示せず）での音楽再生を可能とする所定の処理を行うための着脱可能なメモリカード110を装着する。携帯電話機10
15 0は、さらに、再生された音楽を携帯電話ユーザ1が聴取するためのヘッドホン130を接続可能な構成を有している。

著作権の存在する音楽データをユーザ側で再生可能とするための情報を管理するライセンスサーバ10は、所定の暗号方式により、上記暗号化音楽データを復
20 号するためのコンテンツ復号キーおよび著作権者の側で予め音楽再生に対する制限を指示するためのライセンス情報データを暗号化したうえで、配信するための配信キャリアである携帯電話会社20に対して、このような暗号化したライセンス情報データを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザの携帯電話機100、メモリカード110

が正規の機器であるか否かの承認を行なう。

携帯電話会社 20 は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をライセンスサーバ 10 に中継する。ライセンスサーバ 10 は、配信リクエストがあると、認証サーバ 12 によりユーザの携帯電話機とメモリカードが正規の機器であることを確認し、要求されたライセンス情報データ等を暗号化した上で、携帯電話会社 20 の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

以下では、このようなライセンスサーバ 10 と認証サーバ 12 と携帯電話会社 20 とを併せて、配信サーバ 30 と総称することにする。

また、このような配信サーバ 30 から、各携帯電話端末等にライセンス情報データ等を伝送する処理を「配信」と称することとする。

このような構成とすることで、このデータ配信システムにおいて著作権保護が可能な正規な携帯電話機（コンテンツデータ再生装置）とメモリカードに対してのみ、ライセンス情報データを配信サーバ 30 から受けとって、配布された音楽データの再生が可能となる。

しかも、配信キャリア 20 において、例えば 1 曲分のライセンス情報データを配信する度にその度数を計数しておくことで、著作権料を含む復号情報データの料金を、携帯電話会社 20 が該当携帯電話における通話料金の徴収時に併せて徴収することとすれば、著作権者が著作権料を確保することが容易となる。

図 1 に示したような構成においては、暗号化して配信される音楽データ（コンテンツデータ）をユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、音楽コンテンツデータを暗号化する方式そのものであり、さらに第 2 には、音楽再生における暗号化鍵を配送するための方式であり、さらに、第 3 には、このようにして配信されたデータの無制限な再生等を防止するためのデータ保護を実現する構成である。

[暗号／復号鍵の構成]

図 2 は、図 1 に示したデータ配信システムにおいて使用される通信のための鍵やライセンス情報データ等の特性をまとめて説明するための図である。なお、以下で説明する鍵のうち、「K P」で始まるものは公開鍵である。

まず、図1に示した構成において、CD-ROM200に記録されるデータとしては、音楽データDataと音楽データに関する著作権関連情報あるいはサーバへのアクセス関連情報等の付加情報データData-infとがある。

5 音楽データDataは、後に説明するコンテンツ復号キーKcにより復号可能な暗号化を施した暗号化音楽データ{Data}KcとしてCD-ROM200に記録されるのに対し、付加情報データData-infは平文の状態で記録されている。ここで、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号に変換した情報であることを示している。

10 また、付加情報データData-infには、音楽データDataを識別するためのコードであるコンテンツIDが含まれている。コンテンツIDは、例えば、音楽データDataを演奏するアーティスト名、その曲名などに応じて定められるコードである。

さらに、配信サーバ30において、保持・発生される鍵等としては、音楽データを再生するための復号鍵であるコンテンツ復号キーKcと、メモリカード110内に記録されたコンテンツ復号キーKc等に対するアクセスに対して、例えば、再生回数の制限を指示するための第1の制御情報データAC1と、携帯電話機100等のデータ再生装置に対する再生条件を指定するための第2の制御情報データAC2と、システム共通の公開認証鍵Kpmaと、配信サーバ30からのライセンス情報データ等の配信ごとに更新される固有の共通鍵Ks1と、ライセンスの配信を特定できる管理コードのライセンスIDがある。

ここで、第2の制御情報データAC2により再生条件として指定されるものは、音楽データのうちの1部のみの再生、例えば、曲頭から所定数のフレーズまでの再生を指定したりすることや、再生期限などのデータ再生装置における再生に対して制限を加えるものである。

25 また、ライセンスIDとは、例えば、ある音楽データDataに対するコンテンツ復号キーKc等を、誰に、いつ配信したかを特定するためのコードである。

ライセンス情報データ（復号情報データ）とは、ライセンスID、コンテンツ復号キーKc、第1および第2の制御情報データAC1およびAC2を総称して呼ぶものである。

また、共通鍵 $K_s 1$ は、例えば、ユーザが配信サーバ30に対して1回のアクセスを行なうごとに発生する構成として、1回のアクセスである限り何曲の曲目についても同一の共通鍵 $K_s 1$ が用いられる構成としてもよいし、また、例えば、各曲目ごとにこの共通鍵 $K_s 1$ を変更したうえでその都度ユーザに配信する構成としてもよい。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、このようにセッションごとに更新される共通鍵を「セッションキー」と呼ぶことにする。

再び、図2を参照して、携帯電話機100内のデータ処理を管理するための鍵等としては、携帯電話機100の機種に固有な復号鍵 K_p と、復号鍵 K_p により復号可能な暗号化を行うための公開暗号鍵 K_{Pp} と、再生セッションごとに携帯電話機100内で発生されるセッションキー K_{s4} とがある。

公開暗号鍵 K_{Pp} は、公開認証鍵 K_{Pma} によって復号することで認証可能な付加データと併せて暗号化された署名付きデータ $\{K_{Pp}\} K_{Pma}$ の形式で携帯電話機100内に保持される。さらに、配信サーバ30と携帯電話機100との間のコンテンツ復号キー K_c や第2の制御情報データ $AC2$ の授受のために、全ての携帯電話機100（データ再生装置）に共通の復号鍵 K_{com} が用いられる。

再び、図2を参照して、メモ리카ード110内のデータ処理を管理するための鍵としては、メモ리카ードごとに異なる秘密復号鍵 $K_{m(i)}$ （ i ：自然数）と、秘密復号鍵 $K_{m(i)}$ により復号可能な暗号化を行うための公開暗号鍵 $K_{Pm(i)}$ と、メモ리카ードという媒体の種類に固有であり、かつ、メモ리카ードの種類等毎に異なる秘密復号鍵 K_{mc} と、秘密復号鍵 K_{mc} により復号可能な暗号化を行うための公開暗号鍵 K_{Pmc} と、配信セッションごとにメモ리카ード110内で発生されるセッションキー K_{s2} と、再生セッションごとにメモ리카ード110内で発生されるセッションキー K_{s3} とがある。

ここで、鍵 $K_{m(i)}$ や鍵 $K_{Pm(i)}$ の表記中の自然数 i は、各メモ리카ードを区別するための番号を表わす。さらに、公開暗号鍵 K_{Pmc} は、認証機能を有する公開認証鍵 K_{Pma} によって復号可能な状態に暗号化された署名付きデー

タ {K P m c} K P m a の形式でメモリカード 1 1 0 内に保持される。

[ライセンスサーバ 1 0 の構成]

図 3 は、図 1 に示したライセンスサーバ 1 0 の構成を示す概略ブロック図である。ライセンスサーバ 1 0 は、暗号化音楽データを復号するための鍵や、付加情報データ等の配信情報を保持するための配信情報データベース 3 0 2 と、各ユーザごとにライセンス情報データの配信回数に従った課金情報を保持するための課金データベース 3 0 4 と、配信情報データベース 3 0 2 および課金データベース 3 0 4 からのデータをデータバス B S 1 を介して受取り、所定の暗号化処理を行なうためのデータ処理部 3 1 0 と、通信網を介して、配信キャリア 2 0 とデータ処理部 3 1 0 との間でデータ授受を行なうための通信装置 3 5 0 とを備える。

データ処理部 3 1 0 は、データバス B S 1 上のデータに応じて、データ処理部 3 1 0 の動作を制御するための配信制御部 3 1 2 と、データ再生装置に共通な復号鍵 K c o m を保持するための鍵保持部 3 1 4 と、配信制御部 3 1 2 に制御されて、配信情報データベース 3 0 2 からのデータ、コンテンツ復号キー K c とデータ再生装置に対する制御情報 A C 2 を鍵 K c o m で暗号化するための暗号化処理部 3 1 6 と、各ユーザのメモリカード、例えば、メモリカード 1 1 0 から送信された暗号化されたデータ {K P m c} K P m a を通信装置 3 5 0 からデータバス B S 2 を介して受けて復号し、公開暗号鍵 K P m c を抽出するための復号部 3 1 8 と、セッションキー K s 1 を発生するためのセッションキー発生部 3 2 0 と、セッションキー発生部 3 2 0 より生成されたセッションキー K s 1 を、復号部 3 1 8 により抽出された公開暗号鍵 K P m c により暗号化して、データバス B S 2 に与えるための暗号化処理部 3 2 2 と、各ユーザの携帯電話においてセッションキー K s 1 により暗号化されたうえで送信されたデータを通信装置 3 5 0 およびデータバス B S 2 を介して受けて、復号処理を行なう復号処理部 3 2 4 と、復号処理部 3 2 4 により抽出された公開暗号鍵 K P m (n) を用いて、配信制御部 3 1 2 に制御されて、暗号化処理部 3 1 6 からのデータをさらに暗号化するための暗号化処理部 3 2 6 と、各ユーザのメモリカードにおいてセッションキー K s 1 により暗号化されたうえで送信されたデータをもとに復号処理部 3 2 4 で抽出されたセッションキー K s 2 により暗号化処理部 3 2 6 の出力をさらに暗号化して、

データバスBS2を介して通信装置350に与える暗号化処理部328とを含む。

[携帯電話機(データ再生装置)の構成]

図4は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

5 携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS3と、データバスBS3を介して携帯電話機100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100に与えるためのタッチキー部1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データバスBS3を介して与えられる受信データに基づいて音声を再生するための音声再生部1112と、外部との間でデータの授受を行なうためのコネクタ1120と、コネクタ1120からのデータをデータバスBS3に与え得る信号に変換し、または、データバスBS3からのデータをコネクタ1120に与え得る信号に変換するための外部インターフェース部1122とを備える。

15 携帯電話機100は、さらに、配信サーバ30からのコンテンツ復号キーKc等を記録するための着脱可能なメモ리카ード110と、メモ리카ード110とデータバスBS3との間のデータの授受を制御するためのメモリアンタフェース1200と、データ再生装置としての携帯電話機100に固有の公開暗号鍵Kppを公開認証鍵Kpmaにて復号することにより認証できるように暗号化された署名付きデータ{Kpp} Kpmaとして保持する鍵保持部1204と、鍵Kppにより暗号化されたデータを復号可能な復号鍵Kpを保持するための鍵保持部1210と、メモ리카ード110からデータバスBS3を介して与えられ、鍵Kppで暗号化されているメモ리카ードで発生されたセッションキーKs3を復号鍵Kpで復号するための復号処理部1212と、メモ리카ード110と携帯電話機100の他の部分とのデータ授受にあたり、データバスBS3上においてやり取りされるデータを暗号化するためのセッションキーKs4を乱数等により発生す

るセッションキー発生部1502と、セッションキー発生部1502により生成されたセッションキーKs4を復号処理部1212で抽出されたセッションキーKs3で暗号化して、データバスBS3に与えるための暗号化処理部1504と、データバスBS3上のデータをセッションキーKs4により復号して出力する復号処理部1506と、復号鍵Kcomを保持するための鍵保持部1510と、復号処理部1506の出力を受けて、鍵Kcomで復号してコンテンツ復号キーKcと第2の制御情報データAC2を抽出するための復号処理部1520と、復号処理部1520からの出力を受けてメモ리카ードから読み出された暗号化音楽データ{Data}Kcを復号するための復号処理部1530と、復号処理部1530からの出力を受けて音楽を再生するための音楽再生部1540と、音楽再生部1540の出力と音声再生部1112の出力とを受けて、通話モードであるか、音楽再生モードであるかに応じて選択的に出力するための切換部1542と、切換部1542の出力を受けて、ヘッドホン130と接続するための接続端子1550とを含む。

なお、図4においては、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

[メモ리카ードの構成]

図5は、図4に示したメモ리카ード110の構成を説明するための概略ブロック図である。

以下では、メモ리카ード110を識別するための番号iは、「1」であるものとする。

メモ리카ード110は、メモリインタフェース1200との間で信号を端子1202を介して授受するデータバスBS4と、公開暗号鍵KPmcをシステム共通の鍵KPmaにより暗号化したデータ{KPmc}KPmaの値を保持し、データバスBS4にデータ{KPmc}KPmaを出力するためのKPmc保持部1302と、メモ리카ード110に対応する秘密復号鍵Kmcを保持するためのKmc保持部1304と、データバスBS4にメモリインタフェース1200から端子1202を介して与えられるデータから、秘密復号鍵Kmcにより復号処

理をすることにより、配信サーバ30からのセッションキーKs1を抽出する復号処理部1306と、公開暗号鍵Kpm(1)を保持するためのKpm(1)保持部1310と、発生の都度異なるセッションキーを乱数等により発生するためのセッションキー発生部1312と、セッションキー発生部1312からの出力とKpm(1)保持部1310とを受けて選択的に出力するための切換スイッチ1314と、切換スイッチ1314の出力とデータバスBS5上のデータとを受けて選択的に出力するための切換スイッチ1330と、配信サーバ30からのセッションキーKs1または携帯電話機100からのセッションキーKs4のうち、切換スイッチ1320を介して与えられるいずれか一方に基づいて、切換スイッチ1330からの出力を暗号化してデータバスBS4に与えるための暗号化処理部1340とを備える。

メモ리카ード110は、さらに、システム共通の公開認証鍵Kpmaを保持するためのKpma保持部1350と、Kpma保持部1350からの出力に基づいて、データバスBS4を介して与えられるデータを復号化し、携帯電話機100からの公開暗号鍵Kppを抽出する復号処理部1352と、復号処理部1352により抽出された公開暗号鍵Kppに基づいてセッションキー発生部1352の出力を暗号化してデータバスBS4に与えるための暗号化処理部1354と、データバスBS4上のデータをセッションキー発生部1312からのセッションキーKs2またはKs3により復号処理してデータバスBS5に与えるための復号処理部1356と、鍵Kcomとメモ리카ードごとに異なる公開暗号鍵Kpm(1)とで2重に暗号化されているコンテンツ復号キーKc、付加情報等のデータをデータバスBS5から受理して格納し、かつ、データバスBS4からコンテンツ復号キーKcにより暗号化されている暗号化音楽データ{Data}Kcを受けて格納するためのメモリ1410とを備える。

切換えスイッチ1320は、接点Pa、Pbを有し、接点Paには復号処理部1306からの出力であるセッションキーKs1が与えられ、接点Pbには復号処理部1356からの出力であるセッションキーKs4が与えられる。切換えスイッチ1320は、それぞれ、接点PaとPbに与えられる信号を、動作モードが、「配信モード」と「再生モード」のいずれであるかに応じて、選択的に暗号

化処理部 1 3 4 0 に与える。

一方、切換えスイッチ 1 3 3 0 は、接点 P c、P d を有し、接点 P c には切換
スイッチ 1 3 1 4 からの出力であるセッションキー発生部 1 3 1 2 の出力または
K P m (1) 保持部 1 3 1 0 からの出力が与えられ、接点 P d には、コンテンツ
5 復号キー K c および第 2 の制御情報データ A C 2 データが鍵 K c o m で暗号化さ
れたデータ {K c / / A C 2} K c o m がデータベース B S 5 から与えられる。切
換えスイッチ 1 3 3 0 は、それぞれ、接点 P c と P d に与えられる信号を、動作
モードが、「配信モード」と「再生モード」のいずれであるかに応じて、選択的
に暗号化処理部 1 3 4 0 に与える。

10 メモリカード 1 1 0 は、さらに、秘密復号鍵 K m (1) の値を保持するための
K m (1) 保持部 1 4 1 4 と、少なくとも公開暗号鍵 K P m (1) により暗号化
されたコンテンツ復号キー K c および第 1 の制御情報データ A C 1、第 2 の制御
情報データ A C 2 等を、秘密復号鍵 K m (1) により復号処理してデータベース B
S 5 に与える復号処理部 1 4 1 6 と、ライセンスを購入するための配信動作にお
15 いて、データベース B S 5 上に復号処理部 1 4 1 6 から出力されたデータ {K c /
/ A C 2} K c o m を鍵 K P m (1) で暗号化してメモリ 1 4 1 0 に与えるため
の暗号化処理部 1 4 1 8 と、外部とはデータベース B S 4 を介してデータの授受を
行い、データベース B S 5 から、ライセンス I D、コンテンツ I D、第 1 の制御情
報データ A C 1 等のデータを受けて、メモリカード 1 1 0 の動作を制御するた
め
20 のコントローラ 1 4 2 0 と、データベース B S 5 を介してデータの授受を行い、ラ
イセンス I D、コンテンツ I D、第 1 の制御情報データ A C 1 等のデータの格納
が可能なライセンス情報保持部 1 5 0 0 とを備える。

ここで、{Y / / Z} X という表記は、データ Y と Z とを、鍵データ X により
復号可能な暗号に変換した情報であることを示している。

25 ライセンス情報保持部 1 5 0 0 は、特に限定されないが、例えば、メモリ 1 4
1 0 に格納する音楽データにそれぞれ対応する複数のレジスタを含む。

なお、図 5 において実線で囲んだ領域は、メモリカード 1 1 0 内において、外
部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊
により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化

するためのモジュールTRMに組込まれているものとする。

このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

もちろん、メモリ1410も含めて、モジュールTRM内に組み込まれる構成としてもよい。しかしながら、図5に示したような構成にすると、メモリ1410中に保持されているデータは、いずれも暗号化されているため、このデータのみでは、音楽を再生することはできない。結局、高価なタンパーレジスタンスモジュール内にメモリ1410を設ける必要がないので、製造コストが低減されるという利点がある。

10 [CD-ROMからのデータ複製動作]

図6は、図1および図3～図5で説明したデータ配信システムにおけるCD-ROM200からのデータ複製動作を説明するためのフローチャートである。

図6においては、CD-ROM200はパーソナルコンピュータのCD-ROMドライブにセットされ、パーソナルコンピュータと携帯電話機100とはコネクタ1120を介して接続されているものとする。

まず、パーソナルコンピュータのキーボードからユーザがデータ複製リクエストを与える (ステップS102)。

パーソナルコンピュータは、CD-ROM200から暗号化音楽データ {Data} Kcおよび付加情報データ Data-infを取得して、携帯電話機100にコネクタ1120を介して送信する (ステップS104)。

携帯電話機100が暗号化音楽データ {Data} Kcおよび付加情報データ Data-infを受信すると (ステップS106)、これらのデータは、メモ리카ード110のメモリ1410に格納される (ステップS108)。

メモ리카ード110へのデータの格納が終了すると、携帯電話機100は、パーソナルコンピュータに対して、データ受理の完了を送信する (ステップS110)。

パーソナルコンピュータは、携帯電話機100からの「データ受理」を受信すると (ステップS112)、処理を終了する (ステップS114)。

[ライセンスの購入動作 (配信動作)]

図7および図8は、図1および図3～図5で説明したデータ配信システムにおいて、暗号化音楽データを再生するためのライセンス情報データ等を携帯電話網を介して携帯電話網20を介して携帯電話機100に配信する動作を説明するための第1および第2のフローチャートである。

5 図7および図8においては、携帯電話機100を用いてメモリカード110に対して、ライセンスサーバ10からライセンス情報データの配信を受ける場合の動作を説明している。

まず、配信処理が開始されると（ステップS200）、携帯電話機100から、ユーザによりタッチキー部1108のキーボタンの操作等によって、ライセンス
10 配信リクエストがなされる（ステップS202）。

メモリカード110においては、この配信リクエストに応じて、すでにCD-ROM200から読み込んでいる暗号化音楽データに対応する付加情報データData-infが出力される（ステップS204）。

携帯電話機100においては、付加情報データData-infから配信を受けたいコンテンツを指定するためのコンテンツIDとライセンスサーバ10の電話番号を取得し（ステップS206）、ライセンスサーバ10に対してダイヤルする（ステップS208）。

メモリカード110は、KPMc保持部1302から、復号することで認証できるように暗号化された署名付きデータ{KPMc}KPMaを携帯電話機100
20 に対して送信する（ステップS210）。

携帯電話機100では、メモリカード110から取得したコンテンツID、署名付きデータ{KPMc}KPMaならびに携帯電話機100の鍵保持部1204からの署名付きデータ{KPr}KPMa、さらにユーザ側からのライセンスに対する要求を示す情報ACとが、配信サーバ30に対して送信される（ステップS212）。

ここで、情報ACとしては、例えば、所定回数の再生を許可することの要求や、あるいは、無制限に再生可能とすることを要求するなど、ライセンスの購入形態に対する要求の情報が含まれる。

ライセンスサーバ10では、携帯電話機100から転送されたコンテンツID、

署名付きデータ {K P m c} K P m a ならびに {K P p} K P m a、情報 A C を受信すると (ステップ S 2 1 4)、復号処理部 3 1 8 が、受信した署名付きデータ {K P m c} K P m a ならびに {K P p} K P m a をそれぞれ公開認証鍵 K P m a に基づいて復号し、公開暗号鍵 K P m c および K P p を受取する (ステップ S 2 1 8)。

さらに、ライセンスサーバ 1 0 では、取得した鍵 K P m c および K P p に基づいて認証サーバ 1 2 に対して照会を行ない (ステップ S 2 1 8)、正規携帯電話およびメモリカードを用いたアクセスの場合は次の処理に移行し (ステップ S 2 2 0)、正規携帯電話およびメモリカードでない場合には、処理を終了する (ステップ S 2 5 6)。

照会の結果、正規携帯電話機およびメモリカードであることが確認されると、ライセンスサーバ 1 0 では、セッションキー発生部 3 2 0 が、セッションキー K s 1 を生成する。さらに、ライセンスサーバ 1 0 内の暗号化処理部 3 2 2 が、受信した公開暗号鍵 K P m c により、このセッションキー K s 1 を暗号化してデータ {K s 1} K m c を生成し、通信装置 3 5 0 は、暗号化処理部 3 2 2 からの暗号化データ {K s 1} K m c を、通信網を通じて、携帯電話機 1 0 0 に対して送信する (ステップ S 2 2 0)。

携帯電話機 1 0 0 が、データ {K s 1} K m c を受信すると (ステップ S 2 2 2)、メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 3 0 6 が、秘密復号鍵 K m c により復号処理することにより、セッションキー K s 1 を復号し抽出する (ステップ S 2 2 4)。

続いて、配信動作においては、切換スイッチ 1 3 2 0 は、接点 P a が閉じる状態が選択されており、暗号化処理部 1 3 4 0 は、接点 P a を介して復号処理部 1 3 0 6 からセッションキー K s 1 を受け取る。さらに、セッションキー発生部 1 3 1 2 は、セッションキー K s 2 を発生する。暗号化処理部 1 3 4 0 は、切換スイッチ 1 3 1 4 および 1 3 3 0 を介して、このセッションキー K s 2 と K P m (1) 保持部 1 3 1 0 から与えられる公開暗号鍵 K P m (1) とを受け、セッションキー K s 1 により暗号化し、データ {K s 2 / / K P m (1)} K s 1 を生

成する（ステップS 2 2 6）。

携帯電話機100は、暗号化処理部1340により暗号化されたデータ {K s 2 // K P m (1)} K s 1を配信サーバ30に対して送信する（ステップS 2 2 8）。

5 ライセンスサーバ10では、通信装置350によりデータ {K s 2 // K P m (1)} K s 1が受信され、データバスB S 2に与えられたデータ {K s 2 // K P m (1)} K s 1を復号処理部324が、セッションキーK s 1により復号処理して、セッションキーK s 2および公開暗号鍵K P m (1)を復号抽出する（ステップS 2 3 0）。

10 続いて、配信制御部312は、コンテンツID、情報ACに応じて、配信情報データベース302等に保持されているデータを元に、ライセンスID、第1の制御情報データAC1、第2の制御情報データAC2を生成する（ステップS 2 3 2）。

さらに、ライセンスサーバ10は、コンテンツ復号キーK cを配信情報データベース302より取得する（ステップS 2 3 4）。

15 ライセンスサーバ10では、暗号化処理部316が、コンテンツ復号キーK cと第2の制御情報データAC2とを鍵K c o mで暗号化し、データ {K c // A C 2} K c o mを生成する（ステップS 2 3 6）。さらに、配信サーバ30では、暗号化処理部326が、データ {K c // A C 2} K c o m、ライセンスID、
20 コンテンツIDおよび第1の制御情報データAC1を鍵K P m (1)により暗号化して、データ { {K c // A C 2} K c o m // ライセンスID // コンテンツID // A C 1} K m (1)を生成する（ステップS 2 3 8）。

さらに、暗号化処理部328は、データ { {K c // A C 2} K c o m // ライセンスID // コンテンツID // A C 1} K m (1)をセッションキーK s 2で暗号化して、データ { { {K c // A C 2} K c o m // ライセンスID // コンテンツID // A C 1} K m (1)} K s 2を生成し、通信装置350を介して、携帯電話機100に送信する（ステップS 2 4 0）。

携帯電話機100がデータ { { {K c // A C 2} K c o m // ライセンスID // コンテンツID // A C 1} K m (1)} K s 2を受信すると（ステップ

S 2 4 2)、メモ리카ード110においては、受信したデータ { { {K c / / A C 2} K c o m / / ライセンス I D / / コンテンツ I D / / A C 1} K m (1) } K s 2 を、まず、復号処理部1356が復号処理して、データ { {K c / / A C 2} K c o m / / ライセンス I D / / コンテンツ I D / / A C 1} K m (1) を受領する (ステップS 2 4 4)。

続いて、メモ리카ード110では、復号処理部1416が、データ { {K c / / A C 2} K c o m / / ライセンス I D / / コンテンツ I D / / A C 1} K m (1) を秘密復号鍵K m (1) により復号し、データ {K c / / A C 2} K c o m、ライセンス I D、コンテンツ I D、第1の制御情報データA C 1を受領する (ステップS 2 4 6)。

ライセンス I D、コンテンツ I D、第1の制御情報データA C 1は、ライセンス情報保持部1500に格納され、データ {K c / / A C 2} K c o mは、ふたび暗号化処理部1418により公開暗号鍵K P m (1) により暗号化されて、データ { {K c / / A C 2} K c o m} K m (1) として、メモリ1410に格納される (ステップS 2 4 8)。

メモリ1410へのデータ { {K c / / A C 2} K c o m} K m (1) の格納が終了すると、携帯電話機100は、配信サーバ30に対して「配信受理」を送信する (ステップS 2 5 0)。

ライセンスサーバ10が「配信受理」を受信すると (ステップS 2 5 2)、配信サーバ30において、課金データベース304に携帯電話機100の所有者に対して課金データを格納する等の配信終了処理 (ステップS 2 5 4) が行われ、配信処理が終了する (ステップS 2 5 6)。

以上のような動作により、メモ리카ード110とライセンスサーバ10の間では、それぞれが発生したセッションキーにより、授受するデータを暗号化した上でライセンス情報データの配信を行うことができ、メモ리카ード110は、音楽データを再生可能な状態となる。

なお、以上の説明においては、ステップS 2 1 2～S 2 1 8において、携帯電話機100の鍵保持部1204からの署名付きデータ {K P p} K P m a によりサーバが認証処理を行うものとしたが、たとえば、配信を受ける端末とデータ再

生を行う装置とが一致するとは限らないシステムでは、メモ리카ード側の署名付きデータ {K P m c} K P m a による認証処理だけを残して、署名付きデータ {K P p} K P m a による認証処理を省略することも可能である。

〔再生動作〕

- 5 図9は、携帯電話機100内において、メモ리카ード110に保持された暗号化音楽データ {D a t a} K c から、音楽データを復号化し、復号した音楽データから音楽を再生するための再生処理を説明するフローチャートである。

- 10 図9を参照して、再生処理が開始されると（ステップS300）、携帯電話機100のタッチキー部1108等からのユーザ1の指示により、再生リクエストが与えられると（ステップS302）、携帯電話機100からは、鍵保持部1204から署名付きデータ {K P p} K P m a がメモ리카ード110に対して出力される（ステップS304）。

メモ리카ード110においては、このデータ {K P p} K P m a を復号処理部1352において復号して鍵K P p を受領する（ステップ306）。

- 15 さらに、ステップS306の復号結果に基づいて、鍵K P p が正規の携帯電話機から提供されたものか否かを判断する（ステップS308）。すなわち、署名付きデータ {K P p} K P m a は、公開認証鍵K P m a にて復号する際に発生する付加データの結果によって、鍵K P p が正規のものか否かを判断できる証明機能を有しており、この結果に基づいて判断する。承認不可能と判断した場合は、処理を20 終了する（ステップS336）。

承認可能である場合、続いて、メモ리카ード110のセッションキー発生部1312はセッションキーK s 3 を発生し、このセッションキーK s 3 を暗号化処理部1354が、抽出されている公開暗号鍵K P p により暗号化してデータ {K s 3} K p を生成し、携帯電話機100に対して出力する（ステップS310）。

- 25 承認可能と判断され、メモ리카ード110からデータ {K s 3} K p が送信された場合、携帯電話機100では、メモ리카ード110からのデータ {K s 3} K p を受信すると、復号処理部1212が復号してセッションキーK s 3 を受領する（ステップS312）。

携帯電話機100のセッションキー発生部1502が、セッションキーK s 4

を生成し、暗号化処理部1504が、セッションキーKs3により、セッションキーKs4を暗号化してデータ{Ks4}Ks3を生成し、データバスBS3を介して、メモ리카ード110に対して出力する(ステップS314)。

5 メモ리카ード110は、データバスBS3を介して、携帯電話機100により生成され、かつ暗号化されたセッションキー{Ks4}Ks3を受け取り、復号処理部1356がセッションキーKs3により復号し、セッションキーKs4を抽出する(ステップS316)。

10 さらに、メモ리카ード110では、コントローラ1420は、ライセンス情報保持部1500に保持される第1の制御情報データAC1に基づいて、再生可能なデータに対するリクエストであるか、さらに再生可能なデータに対するリクエストのときに再生回数の制限があるかを判断する(ステップS308)。再生可能であって再生回数に制限がある場合、ライセンス情報保持部1500内の第1の制御情報データAC1の内容を更新する、すなわち、残りの再生回数が1回分減るように、第1の制御情報データAC1の内容を更新する(ステップS319)。
15 一方、再生可能であって再生回数に制限がないと判断した場合は、処理はステップS320に移行する。さらに、再生不可能と判断した場合は、処理を終了する(ステップS336)。

20 続いて、メモ리카ード110は、メモリ1410から、再生リクエスト曲に対応する暗号化されているデータ{{Kc//AC2}Kcom}Km(1)を読み出し、復号処理部1416が復号処理を行ない、データ{Kc//AC2}Kcomが取得される(ステップS320)。

25 さらに、暗号化処理部1340は、切換スイッチ1320を介して復号処理部1356から与えられたセッションキーKs4により、切換スイッチ1330を介してデータバスBS5から与えられるデータ{Kc//AC2}Kcomを暗号化してデータバスBS4およびBS3を介して、携帯電話機100に出力する(ステップS322)。

携帯電話機100の復号処理部1506は、セッションキーKs4により復号化処理を行なうことにより、データ{Kc//AC2}Kcomを取得する(ステップS324)。さらに、復号処理部1520が復号処理することにより、コ

ンテンツ復号キーK c および第2の制御情報データAC 2が抽出される（ステップS 3 2 6）。

携帯電話機1 0 0のコントローラ1 1 0 6は、第2の制御情報データAC 2の内容を確認し（ステップS 3 2 8）、再生不可能の場合は、処理を終了する（ステップS 3 3 6）。

一方、再生可能な場合には、携帯電話機1 0 0のコントローラ1 1 0 6は、メモ리카ード1 1 0を制御して、メモ리카ード1 1 0のメモリ1 4 1 0に格納されている再生リクエスト曲に対応する暗号化されたコンテンツデータ {D a t a} K c を読出し、出力させる（ステップS 3 3 0）。

10 携帯電話機1 0 0の音楽再生部1 5 4 0は、暗号化コンテンツデータ {D a t a} K c を、抽出されたコンテンツ復号キーK c により復号処理して平文の音楽データを生成し（ステップS 3 3 2）、コンテンツデータを再生して切換部1 5 4 2に与える（ステップS 3 3 4）。切換部1 5 4 2は、外部に再生された音楽を出力し、処理が終了する（ステップS 3 3 6）。

15 なお、ステップS 3 0 4～S 3 1 2の処理は、再生動作ごとに行う必要は必ずしもなく、メモ리카ード挿入時または電源投入時に行う処理としてもよい。

このような構成とすることで、携帯電話等の情報通信網を介してデータの授受を行なうことが可能なユーザに対して、著作権を保護しつつ、簡易に音楽コンテンツ情報の供給を行ない、かつ、ユーザは短時間で音楽の再生を行うことが可能となる。

20 しかも、配信されたライセンス（復号）情報データが、著作権者の許可なく無制限に再生されたり複製されることを防止することが可能となる。

なお、以上の説明では、鍵K c o mは共通鍵であるものとして説明したが、この鍵K c o mによる暗号化処理に対応する処理を、公開鍵方式に変更することも可能である。この場合は、暗号化鍵が公開鍵となり、公開暗号鍵K P c o mをライセンスサーバ1 0の側で使用し、秘密復号鍵K c o mを再生回路である携帯電話機1 0 0の側で使用するようになる。

また、以上の実施例1の説明では、ライセンス情報データ（ライセンスID、コンテンツ復号キーK c、第1および第2の制御情報データAC 1およびAC

2) のうち、コンテンツ復号キー Kc および第 2 の制御情報データ AC 2 は、暗号化を施された上で、メモリ 1410 に記録されるものとした。しかしながら、本発明はこのような場合に限定されることなく、メモリカード内で暗号化し直さずに、ライセンス情報データの全てをライセンス情報保持部 1500 に格納する構成とすることも可能である。このような構成とすれば、再生開始までのオーバーヘッド時間を短縮することが可能であり、また、メモリカード内のコントローラを制御するソフトウェアを簡略化できるなどの利点がある。

したがって、実施例 1 の構成において、ライセンス情報データの全てをライセンス情報保持部 1500 に格納する場合には、まず、図 5 に示したメモリカード 110 の構成において、暗号化処理部 1418 が不要となる。さらに、図 8 に示したステップ S 248 における処理を、「データ {Kc / / AC 2} Kcom、ライセンス ID、コンテンツ ID、第 1 の制御情報データ AC 1 を、ライセンス情報保持部 1500 に格納する」と変更する。さらに、図 9 において、ステップ S 320 を、「ライセンス情報保持部 1500 に格納されている再生リクエスト曲の {Kc / / AC 2} Kcom を取得」に変更すれば良い。

さらに、メモリカード内の機構が、1 チップ LSI で構成されている場合などは、メモリ 1410 自身も TRM 内に形成されることになる。このような場合は、ライセンス情報保持部 1500 としてメモリ 1410 の一部を割当て、このようにして割当てられたライセンス情報保持部 1500 に、データ {Kc / / AC 2} Kcom、ライセンス ID、コンテンツ ID、第 1 の制御情報データ AC 1 を格納することも可能である。

[実施例 1 の変形例]

図 1 に示した実施例 1 のデータ配信システムの構成においては、CD-ROM 200 からメモリカード 110 への暗号化音楽データおよび付加情報データの書込みにおいては、パーソナルコンピュータを介してコネクタ 1120 から携帯電話機 100 経由で、データの書込みを行っていた。

しかしながら、たとえば、パーソナルコンピュータに接続された汎用のメモリカードドライブ装置により、CD-ROM からメモリカード 110 に暗号化音楽データ等を取り込む構成とすることも可能である。その他の構成については、実

施例 1 と同様であるので、その説明は省略する。

このような構成のデータ配信システムでも実施例 1 と同様の効果を奏することが可能である。

〔実施例 2〕

5 図 10 は、本発明の実施例 2 のデータ配信システムの構成を示す概念図である。
図 1 に示した実施例 1 のデータ配信システムの構成と異なる点は、CD-ROM
200 からメモ리카ード 110 への暗号化音楽データおよび付加情報の書込みに
おいて、パーソナルコンピュータを介してコネクタ 1120 から携帯電話機 10
0 経由でデータを書込む代わりに、パーソナルコンピュータに接続された専用の
10 メモ리카ードドライブ装置 500 により、CD-ROM 200 からメモ리카ード
110 に暗号化音楽データ等を書込む構成となっている点である。その他の点は、
実施例 1 のデータ配信システムを同様であるので、同一部分には、同一符号を付
して、その説明は繰り返さない。

ここで、後の説明で明らかとなるように、実施例 2 のメモ리카ードドライブ装
15 置 500 は、実施例 1 の変形例で述べたような汎用のメモ리카ードドライブ装置
の構成とは異なり、メモ리카ードとの間で授受するデータに対する暗号化処理お
よび復号処理に対応するための構成を有する。

図 11 は、図 10 に示したメモ리카ードドライブ装置 500 の構成を示す概略
ブロック図である。以下では、メモ리카ードドライブ装置 500 内でセッション
20 ごとに生成されるセッションキーを $K_s 5$ とする。

図 11 を参照して、メモ리카ードドライブ装置 500 は、パーソナルコンピュ
ータとの間でデータの授受を行なうためのコネクタ 2120 と、コネクタ 212
0 からのデータをメモ리카ードドライブ装置 500 の内部に与え得る信号に変換
し、または、メモ리카ードドライブ装置 500 の内部からのデータをコネクタ 2
25 120 に与え得る信号に変換するための外部インターフェース部 2122 と、外
部インターフェース 2122 からのデータに応じて、メモ리카ードドライブ装置
500 の動作を制御するためのコントローラ 2124 とを備える。

メモ리카ードドライブ装置 500 は、さらに、メモ리카ード 110 とデータバ
ス BS 6 との間のデータの授受を制御するためのメモリアンタフェース 2200

と、システムに共通な公開認証鍵 $K P m a$ を保持する鍵保持部2204と、データベースBS6から与えられ公開認証鍵 $K P m a$ により暗号化されたデータを復号するための復号処理部2206と、メモリカード110とメモリカードドライブ装置500の他の部分とのデータ授受にあたり、データベースBS6上においてやり取りされるデータを暗号化するためのセッションキー $K s 5$ を乱数等により発生するセッションキー発生部2210と、セッションキー発生部2210により生成されたセッションキー $K s 5$ を復号処理部2206で抽出された公開暗号鍵 $K P m c$ で暗号化して、データベースBS6に与えるための暗号化処理部2208と、データベースBS6上のデータをセッションキー $K s 5$ により復号して出力する復号処理部2212と、復号処理部2212の出力を受けて、データベースBS6からのデータを公開暗号鍵 $K P m (1)$ で暗号化するための暗号化処理部2214と、暗号化処理部2214の出力を受けて復号処理部2212で抽出されたセッションキー $K s 2$ で暗号化するための暗号化処理部2216と、メモリカードドライブ装置500に固有の複数の鍵 $K c d (j)$ (j :自然数)を保持する $K c d (j)$ 保持部2222と、複数の鍵 $K c d (j)$ のうちの選択されたものでデータベースBS6上のデータを復号するための $K c d$ 復号部2220とを含む。

[データの複製動作]

図12および図13は、図10および図11で説明したデータ配信システムにおいて、CD-ROM200からメモリカード110へ暗号化音楽データを複製する動作を説明するための第1および第2のフローチャートである。

メモリカード110は、実施例1と同様の構成を有する。以下の説明で明らかとなるように、CD-ROM200からメモリカード110へのライセンス情報データの転送が行われるためには、まず、CD-ROM200とメモリカードドライブ装置500との間で認証が行われることが必要である。さらに、メモリカードドライブ装置500は、CD-ROM200内のデータがライセンス対応データの場合、メモリカード110と所定の方式にしたがって、データの授受が可能である場合にのみ、すなわち、メモリカード110がこのデータ配信システムに適合する構成を有している場合にのみ、CD-ROM200からメモリカード110へのライセンス情報データの複製を可能とするものである。言いかえると、

メモ리카ードドライブ装置 500 がメモ리카ード 110 に対して擬似的に配信サーバとして正規に動作し得るかに応じて、メモ리카ードの認証が行われる。

したがって、以下の説明では、メモ리카ード 110 とメモ리카ードドライブ装置 500 との間で授受されるライセンス ID は仮のものであって、これを仮ライセンス ID IDa とよび、第 1 の制御情報データ AC1、第 2 の制御情報データ AC2 も制限付のコードであることを示すために、それぞれ記号 AC1a、AC2a で表すことにする。ここで、ユーザは、このような制限のないライセンス情報データを欲するのであれば、サーバから別途配信を受ければよい。

図 12 および図 13 においては、CD-ROM 200 からメモ리카ード 110 へ音楽データを複製する場合の動作を説明している。

まず、複製処理が開始されると（ステップ S400）、パーソナルコンピュータのキーボタンの操作等によって、データ複製リクエストがなされる（ステップ S402）。

パーソナルコンピュータは、CD-ROM 200 よりクラス ID データを取得する（ステップ S404）。このクラス ID データにより、Kcd(j) 保持部 2222 中の 1 つのキー Kcd(j) が特定されるものとする。

メモ리카ードドライブ装置 500 は、クラス ID に基づいて、CD-ROM 200 がカードドライブ装置 500 に対応できるか否かの判断を行う（ステップ S406）。

CD-ROM 200 がカードドライブ装置 500 に対応できない場合、処理はステップ S432 に移行する。

一方、CD-ROM 200 が対応できる場合、メモ리카ード 110 は、KPMC 保持部 1302 から、暗号化された署名付きデータ {KPMC} KPMa をメモ리카ードドライブ装置 500 に対して送信する（ステップ S408）。

メモ리카ードドライブ装置 500 では、メモ리카ード 110 から転送された署名付きデータ {KPMC} KPMa を受信すると、復号処理部 2206 が、受信した署名付きデータ {KPMC} KPMa を公開認証鍵 KPMa に基づいて復号し、公開暗号鍵 KPMC を受理する（ステップ S410）。

すなわち、メモ리카ードドライブ装置 500 は、メモ리카ード 110 の認証を

行うことになり、認証できなければ、i) 処理を中断する、あるいは、ii) ステップS 4 3 2へ処理を移行させる、のいずれかの処置をとる構成とすることができる。

さらに、メモリカードドライブ装置5 0 0では、セッションキー発生部2 2 1 0が、セッションキーK s 5を生成する。さらに、メモリカードドライブ装置5 0 0内の暗号化処理部2 2 0 8が、受信したキーK P m cにより、このセッションキーK s 5を暗号化してデータ {K s 5} K m cを生成し、メモリカード1 1 0に対して送信する（ステップS 4 1 2）。

メモリカード1 1 0が、データ {K s 5} K m cを受信すると、メモリカード1 1 0においては、復号処理部1 3 0 6が、キーK m cにより復号処理することにより、セッションキーデータK s 5を抽出する（ステップS 4 1 4）。

続いて、メモリカード1 1 0においては、切換スイッチ1 3 2 0は、接点P aが閉じる状態が選択されており、暗号化処理部1 3 4 0は、接点P aを介して復号処理部1 3 0 6からセッションキーK s 5を受け取る。さらに、セッションキー発生部1 3 1 2は、セッションキーK s 2を発生する。暗号化処理部1 3 4 0は、切換スイッチ1 3 1 4および1 3 3 0を介して、このセッションキーK s 2とK P m (1) 保持部1 3 1 0から与えられる公開暗号鍵K P m (1) とを受け、セッションキーK s 5により暗号化し、データ {K s 2//K P m (1)} K s 5を生成し出力する（ステップS 4 1 6）。

メモリカードドライブ装置5 0 0では、データ {K s 2//K P m (1)} K s 5が受信され、データバスB S 6に与えられたデータ {K s 2//K P m (1)} K s 5を復号処理部2 2 1 2が、セッションキーK s 5により復号処理して、セッションキーK s 2および公開暗号鍵K P m (1) を復号抽出する（ステップS 4 1 8）。

続いて、メモリカードドライブ装置5 0 0は、CD-ROM2 0 0に予め記録されているデータ { {K c//AC 2 a} K c o m//ライセンスID a//コンテンツID//AC 1 a} K c d (j) をパーソナルコンピュータ経由で受信し、データ { {K c//AC 2 a} K c o m//ライセンスID a//コンテンツID//AC 1 a} K c d (j) を、まず、復号処理部2 2 1 2が復号処理し

て、データ {Kc//AC2a} Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを取得する（ステップS420）。

ここで、CD-ROM200からのクラスIDデータとキーKcd(j)との間の対応がしていなければ、メモリカードドライブ装置500は、データ {Kc//AC2a} Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを取得できないことになる。

続いて、メモリカードドライブ装置500では、暗号化処理部2214が、データ {Kc//AC2a} Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを公開暗号鍵Kpm(1)により暗号化し、{ {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)を生成する（ステップS422）。

つづいて、メモリカードドライブ装置500では、暗号化処理部2216が、{ {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)をセッションキーKs2により暗号化し、データ { { {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)} Ks2を生成し出力する（ステップS424）。

メモリカード110では、復号処理部1356が、データ { { {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)} Ks2をセッションキーKs2により復号し、データ { {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)を受理する（ステップS426）。

さらに、メモリカード110では、復号処理部1416が、データ { {Kc//AC2a} Kcom//ライセンスIDa//コンテンツID//AC1a} Km(1)を秘密復号鍵Km(1)により復号し、データ {Kc//AC2a} Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを受理する（ステップS428）。

ライセンスIDa、コンテンツID、第1の制御情報データAC1aは、ライセンス情報保持部1500に格納され、データ {Kc//AC2a} Kcomは、ふたたび暗号化処理部1418により公開暗号鍵Kpm(1)により暗号化され

て、データ { {Kc//AC2a} Kcom} Km (1) として、メモリ1410に格納される (ステップS430)。

メモリ1410へのデータ { {Kc//AC2a} Kcom} Km (1) の格納が終了すると、パーソナルコンピュータは、CD-ROM200から暗号化音楽データ {Data} Kcおよび付加情報データData-infをCD-ROM200から取得して、メモリカードドライブ装置500にコネクタ2120を介して送信する (ステップS432)。

メモリカードドライブ装置500が暗号化音楽データ {Data} Kcおよび付加情報データData-infを受信すると (ステップS434)、これらのデータを、メモリカード110のメモリ1410に格納する (ステップS436)。

メモリカード110へのデータの格納が終了すると、メモリカードドライブ装置500は、パーソナルコンピュータに対して、データ受理の完了を送信する (ステップS438)。

パーソナルコンピュータでは、メモリカードドライブ装置500からの「データ受理」を受信すると (ステップS440)、処理が終了する (ステップS442)。

なお、実施例2においても、ライセンスの購入動作 (配信動作) および再生動作は、実施例1と同様に行うことができる。

以上のような動作により、メモリカード110にCD-ROM200からデータを複製することが可能である。しかも、このようにして、メモリカード110に暗号化音楽データが複製された後は、実施例1と同様の効果を奏する。

また、以上の実施例2の説明でも、ライセンス情報データ (ライセンスIDa、コンテンツID、コンテンツ復号キーKc、第1および第2の制御情報データAC1aおよびAC2a) のうち、コンテンツ復号キーKcおよび第2の制御情報データAC2aは、暗号化を施された上で、メモリ1410に記録されるものとした。しかしながら、実施例2においても、実施例1と同様に、メモリカード内で暗号化し直さずに、ライセンス情報データの全てをライセンス情報保持部1500に格納する構成とすることも可能である。

したがって、実施例2の構成において、ライセンス情報データの全てをライセンス情報保持部1500に格納する場合には、図13に示したステップS430における処理を、「データ{Kc//AC2a}Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを、ライセンス情報保持部1500に格納する」と変更する。

さらに、メモリカード内の機構が、1チップLSIで構成されている場合などは、ライセンス情報保持部1500としてメモリ1410の一部を割当て、このようにして割当てられたライセンス情報保持部1500に、データ{Kc//AC2a}Kcom、ライセンスIDa、コンテンツID、第1の制御情報データAC1aを格納することも可能である。

[実施例3]

実施例3のデータ配信システムは、実施例1のデータ配信システムの構成において、携帯電話機（データ再生装置）に共通な鍵Kcomを省略した構成となっている点で異なるものの、その他の点は同様である。

図14は、実施例3のデータ配信システムにおいて使用される通信のためのライセンス情報データ等の特性をまとめて説明するための図であり、実施例1の図2と対比される図である。

上述のとおり、実施例3では、鍵Kcomを省略した構成となっている点で実施例1と異なるのみであるので、その説明は繰り返さない。

図15は、実施例3のライセンスサーバ31の構成を示す概略ブロック図であり、実施例1の図3と対比される図である。

実施例3のライセンスサーバ31では、鍵Kcomを省略した構成となっている点で実施例1のライセンスサーバ10と異なるのみであるので、同一部分には同一符号を付してその説明は繰り返さない。

図16は、実施例3の携帯電話機101の構成を示す概略ブロック図であり、実施例1の図4と対比される図である。

実施例3の携帯電話機101では、鍵Kcomを省略したことに対応して、鍵保持部1510と復号処理部1520とが省略される構成となっている点で実施例1の携帯電話機100の構成と異なるのみであるので、同一部分には同一符号

を付してその説明は繰り返さない。

実施例 3 のデータ配信システムにおける CD-ROM 200 からのデータ複製動作は実施例 1 の動作と同様である。

[ライセンスの購入動作 (配信動作)]

5 図 17 および図 18 は、図 15～図 16 で説明したデータ配信システムにおいて、暗号化音楽データを再生するためのライセンス情報データ等を携帯電話網を介して携帯電話機 101 に配信する動作を説明するための第 1 および第 2 のフローチャートである。

10 図 17 および図 18 においては、ユーザ 1 が、メモリカード 110 に対して、ライセンスサーバ 31 からライセンス情報データの配信を受ける場合の動作を説明している。

まず、配信処理が開始されると (ステップ S500)、ユーザ 1 は携帯電話機 101 から、ユーザによりタッチキー部 1108 のキーボタンの操作等によって、ライセンス配信リクエストがなされる (ステップ S502)。

15 メモリカード 110 においては、この配信リクエストに応じて、すでに CD-ROM 200 から読み込んでいる暗号化音楽データに対応する付加情報データ Data-inf が出力される (ステップ S504)。

携帯電話機 101 においては、付加情報から配信を受けたいコンテンツを指定するためのコンテンツ ID とライセンスサーバの電話番号を取得し (ステップ S506)、ライセンスサーバ 31 に対してダイヤルする (ステップ S508)。

20 メモリカード 110 は、KPmc 保持部 1302 から、データ {KPmc} KPma を携帯電話機 101 に対して出力する (ステップ S510)。

携帯電話機 101 では、メモリカード 110 から取得したコンテンツ ID、データ {KPmc} KPma ならびに携帯電話機 101 の鍵保持部 1204 からのキー {Kpp} KPma、さらにユーザ側からのライセンスに対する要求を示す情報 AC とを、ライセンスサーバ 31 に対して送信する (ステップ S512)。

25 ここで、情報 AC としては、例えば、所定回数の再生を許可することの要求や、あるいは、無制限に再生可能とすることを要求するなど、ライセンスの購入形態に対する要求の情報が含まれる。

ライセンスサーバ31では、携帯電話機100から転送されたコンテンツID、データ{K P m c} K P m aならびにデータ{K P p} K P m a、情報ACを受信すると(ステップS 5 1 4)、復号処理部318が、受信したデータ{K P m c} K P m aならびにデータ{K P p} K P m aを公開認証鍵K P m aに基づいて復号し、鍵K P m cおよびK P pを受理する(ステップS 5 1 8)。

さらに、ライセンスサーバ31では、取得した鍵K P m cおよびK P pに基づいて認証サーバ12に対して照会を行ない(ステップS 5 1 8)、正規の携帯電話機および正規のメモリカードへの配信の場合は次の処理に移行し(ステップS 5 2 0)、正規携帯電話機および正規のメモリカードでない場合には、処理を終了する(ステップS 5 5 6)。

照会の結果、正規携帯電話機およびメモリカードであることが確認されると、ライセンスサーバ31では、セッションキー発生部320が、セッションキーK s 1を生成する。さらに、ライセンスサーバ31内の暗号化処理部322が、受信した公開暗号鍵K P m cにより、このセッションキーK s 1を暗号化してデータ{K s 1} K m cを生成し、通信装置350は、暗号化処理部322からの暗号化データ{K s 1} K m cを、通信網を通じて、携帯電話機101に対して出力する(ステップS 5 2 0)。

携帯電話機101が、データ{K s 1} K m cを受けると(ステップS 5 2 2)、メモリカード110においては、メモリインタフェース1200を介して、データバスB S 3に与えられたデータを、復号処理部1306が、秘密復号鍵K m cにより復号処理することにより、セッションキーデータK s 1を復号し抽出する(ステップS 5 2 4)。

続いて、配信動作においては、切換スイッチ1320は、接点P aが閉じる状態が選択されているので、暗号化処理部1340は、接点P aを介して復号処理部1306からセッションキーK s 1を受け取る。さらに、セッションキー発生部1312は、セッションキーK s 2を発生する。暗号化処理部1340は、切換スイッチ1314および1330を介して、このセッションキーK s 5とK P m (1)保持部1310から与えられる公開暗号鍵K P m (1)とを受け、セッションキーK s 1により暗号化し、データ{K s 2//K P m (1)} K s 1を

生成する（ステップS526）。

携帯電話機101は、暗号化処理部1340により暗号化されたデータ {Ks2//Kpm(1)} Ks1をライセンスサーバ31に対して送信する（ステップS528）。

5 ライセンスサーバ31では、通信装置350によりデータ {Ks2//Kpm(1)} Ks1が受信され、データベースBS2に与えられたデータ {Ks2//Kpm(1)} Ks1を復号処理部324が、セッションキーKs1により復号処理して、セッションキーKs2および公開暗号鍵Kpm(1)を復号抽出する（ステップS530）。

10 続いて、配信制御部312は、コンテンツID、情報ACに応じて、配信情報データベース302等に保持されているデータを元に、ライセンスID、第1の制御情報データAC1、第2の制御情報データAC2を生成する（ステップS532）。

15 さらに、ライセンスサーバ31は、コンテンツ復号キーKcを配信情報データベース302より取得する（ステップS534）。

20 ライセンスサーバ31では、暗号化処理部326が、データ {Kc//AC2} Kcom、ライセンスID、コンテンツIDおよび第1の制御情報データAC1を公開暗号鍵Kpm(1)により暗号化して、データ {Kc//AC2//ライセンスID//コンテンツID//AC1} Km(1)を生成する（ステップS538）。

25 さらに、暗号化処理部328は、データ {Kc//AC2//ライセンスID//コンテンツID//AC1} Km(1)をセッションキーKs2で暗号化して、データ { {Kc//AC2//ライセンスID//コンテンツID//AC1} Km(1)} Ks2を生成し、通信装置350を介して、携帯電話機101に送信する（ステップS540）。

携帯電話機101がデータ { {Kc//AC2//ライセンスID//コンテンツID//AC1} Km(1)} Ks2を受信すると（ステップS542）、メモリカード110においては、受信したデータ { {Kc//AC2//ライセンスID//コンテンツID//AC1} Km(1)} Ks2を、まず、復号処

理部 1 3 5 6 が復号処理して、データ {K c // A C 2 // ライセンス I D // コンテンツ I D // A C 1} K m (1) を受理する (ステップ S 5 4 4)。

5 続いて、メモリカード 1 1 0 では、復号処理部 1 4 1 6 が、データ {K c // A C 2 // ライセンス I D // コンテンツ I D // A C 1} K m (1) を秘密復号鍵 K m (1) により復号し、コンテンツ復号キー K c、第 2 の制御情報データ A C 2、ライセンス I D、コンテンツ I D、第 1 の制御情報データ A C 1 を受理する (ステップ S 5 4 6)。

10 ライセンス I D、コンテンツ I D、第 1 の制御情報データ A C 1 は、ライセンス情報保持部 1 5 0 0 に格納され、コンテンツ復号キー K c および第 2 の制御情報データ A C 2 は、ふたたび暗号化処理部 1 4 1 8 によりキー K P m (1) により暗号化されて、データ {K c // A C 2} K m (1) として、メモリ 1 4 1 0 に格納される (ステップ S 5 4 8)。

15 メモリ 1 4 1 0 へのデータ {K c // A C 2} K m (1) の格納が終了すると、携帯電話機 1 0 1 は、ライセンスサーバ 3 1 に対して「配信受理」を送信する (ステップ S 5 5 0)。

ライセンスサーバ 3 1 が「配信受理」を受信すると (ステップ S 5 5 2)、ライセンスサーバ 3 1 において、課金データベース 3 0 4 に携帯電話機 1 0 1 の契約者の課金データを格納する等の配信終了処理 (ステップ S 5 5 4) が行われ、配信処理が終了する (ステップ S 5 5 6)。

20 以上のような動作により、メモリカード 1 1 0 とライセンスサーバ 3 1 との間では、それぞれが発生したセッションキーにより、授受するデータを暗号化した上で配信動作を行うことができ、メモリカード 1 1 0 は、音楽情報を再生可能な状態となる。

25 なお、以上の説明においても、ステップ S 5 1 2 ~ S 5 1 8 において、携帯電話機 1 0 0 の鍵保持部 1 2 0 4 からの署名付きデータ {K P p} K P m a によりサーバが認証処理を行うものとしたが、たとえば、配信を受ける端末とデータ再生を行う装置とが一致するとは限らないシステムでは、メモリカード側の署名付きデータ {K P m c} K P m a による認証処理だけを残して、署名付きデータ {K P p} K P m a による認証処理を省略することも可能である。

[再生動作]

図19は、携帯電話機101内において、メモ리카ード110に保持された暗号化音楽データ {Data} Kcから、音楽データを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

5 図19を参照して、再生処理が開始されると(ステップS600)、携帯電話のキーボード1108等からのユーザ1の指示により、再生リクエストが与えられると(ステップS602)、携帯電話機101からは、鍵保持部1204から署名付きデータ {KPp} KPmaがメモ리카ード110に対して出力される(ステップS604)。

10 カード110においては、この署名付きデータ {KPp} KPmaを復号処理部1352において復号して公開暗号鍵KPpを受理する(ステップS606)。

承認可能である場合、つづいて、メモ리카ード110のセッションキー発生部1312はセッションキーKs3を発生し、このセッションキーKs3を暗号化処理部1354が、抽出されている公開暗号鍵KPpにより暗号化してデータ

15 {Ks3} KPpを生成し、携帯電話機100に対して送信する(ステップS610)。

復号可能と判断され、カード110からデータ {Ks3} KPpが送信された場合、携帯電話機100では、カード110からのデータ {Ks3} KPpを受信すると、復号処理部1212が復号してセッションキーKs3を受理する(ステップS612)。

20 携帯電話機101のセッションキー発生部1502が、セッションキーKs4を生成し、暗号化処理部1504が、セッションキーKs3により、セッションキーKs4を暗号化してデータ {Ks4} Ks3を生成し、データベースBS3を介して、メモ리카ード110に対して送信する(ステップS614)。

25 メモ리카ード110は、データベースBS3を介して、携帯電話機101により生成され、かつ暗号化されたデータ {Ks4} Ks3を受け取り、復号処理部1356がセッションキーKs3により復号し、セッションキーKs4を抽出する(ステップS616)。

さらに、メモ리카ード110では、コントローラ1420は、ライセンス情報

保持部 1 5 0 0 に保持される第 1 の制御情報データ A C 1 に基づいて、再生可能なデータに対するリクエストであるか、さらに再生可能なデータに対するリクエストのときに再生回数の制限があるかを判断する（ステップ S 6 1 8）。再生可能であって再生回数に制限がある場合、ライセンス情報保持部 1 5 0 0 内の第 1
5 の制御情報データ A C 1 の内容を更新する、すなわち、残りの再生可能回数を示すように、第 1 の制御情報データ A C 1 の内容を更新する（ステップ S 6 1 9）。一方、再生可能であって再生回数に制限がないと判断した場合は、処理はステップ S 6 2 0 に移行する。さらに、再生不可能と判断した場合は、処理を終了する（ステップ S 6 3 6）。

10 続いて、メモ리카ード 1 1 0 は、メモリ 1 4 1 0 から、再生リクエスト曲に対応する暗号化されているデータ {K c / / A C 2} K m (1) を読出し、復号処理部 1 4 1 6 が復号処理を行ない、コンテンツ復号キー K c および第 2 の制御情報データ A C 2 が取得される（ステップ S 6 2 0）。

さらに、暗号化処理部 1 3 4 0 は、切換スイッチ 1 3 2 0 を介して復号処理部
15 1 3 5 6 から与えられたセッションキー K s 4 により、切換スイッチ 1 3 3 0 を介してデータバス B S 5 から与えられるコンテンツ復号キー K c および第 2 の制御情報データ A C 2 を暗号化して、データ {K c / / A C 2} K s 4 をデータバス B S 4 および B S 3 を介して、携帯電話機 1 0 1 に出力する（ステップ S 6 2 2）。

20 携帯電話機 1 0 1 の復号処理部 1 5 0 6 は、セッションキー K s 4 により復号化処理を行なうことにより、コンテンツ復号キー K c および第 2 の制御情報データ A C 2 を取得する（ステップ S 6 2 4）。

携帯電話機 1 0 1 のコントローラ 1 1 0 6 は、第 2 の制御情報データ A C 2 の内容を確認し（ステップ S 6 2 8）、再生不可能の場合は、処理を終了する（ス
25 テップ S 6 3 6）。

一方、再生可能な場合には、携帯電話機 1 0 1 のコントローラ 1 1 0 6 は、メモ리카ード 1 1 0 を制御して、メモ리카ード 1 1 0 のメモリ 1 4 1 0 に格納されている再生リクエスト曲に対応する暗号化された音楽データ {D a t a} K c を読出し、出力させる（ステップ S 6 3 0）。

携帯電話機の音楽再生部 1540 は、暗号化された音楽データ {Data} K_c を、抽出されたコンテンツ復号キー K_c により復号処理して平文の音楽データを生成し (ステップ S632)、音楽を再生して切換部 1542 に与える (ステップ S634)。切換部 1542 は、外部に再生された音楽を出力し、処理が終了する (ステップ S636)。

なお、ステップ S604～S612 の処理は、再生動作ごとに行う必要は必ずしもなく、メモリカード挿入時または電源投入時に行う処理としてもよい。

このような構成によっても実施例 1 と同様に、携帯電話等の情報通信網を介してデータの授受を行なうことが可能なユーザに対して、著作権を保護しつつ、簡易に音楽コンテンツ情報の供給を行ない、かつ、ユーザは短時間で音楽の再生を行うことが可能となる。

しかも、配信された著作物データが、著作権者の許可なく無制限に再生されたり複製されることを防止することが可能となる。

なお、実施例 2 で説明したメモリカードドライブ装置 500 を用いる構成においても、鍵 K_{com} を省略する構成とすることも可能である。

また、以上の実施例 3 の説明でも、ライセンス情報データ (ライセンス ID、コンテンツ復号キー K_c、第 1 および第 2 の制御情報データ AC1 および AC2) のうち、コンテンツ復号キー K_c および第 2 の制御情報データ AC2 は、暗号化を施された上で、メモリ 1410 に記録されるものとした。しかしながら、本発明はこのような場合に限定されることなく、実施例 3 でも、メモリカード内で暗号化し直さずに、ライセンス情報データの全てをライセンス情報保持部 1500 に格納する構成とすることも可能である。

したがって、実施例 3 の構成において、ライセンス情報データの全てをライセンス情報保持部 1500 に格納する場合には、まず、メモリカード 110 の構成において、暗号化処理部 1418 が不要となる。さらに、図 18 に示したステップ S548 における処理を、「コンテンツ復号キー K_c、第 2 の制御情報データ AC2、ライセンス ID、コンテンツ ID、第 1 の制御情報データ AC1 を、ライセンス情報保持部 1500 に格納する」と変更する。さらに、図 19 において、ステップ S320 を、「ライセンス情報保持部 1500 に格納されている再生リ

クエスト曲のコンテンツ復号キーK c および第2の制御情報データAC2を取得」に変更すれば良い。

さらに、メモリカード内の機構が、1チップLSIで構成されている場合などは、ライセンス情報保持部1500としてメモリ1410の一部を割当て、この
5 ようにして割当てられたライセンス情報保持部1500に、ライセンス情報データを格納することも可能である。

さらに、以上の各実施例の説明では、音楽データ等のコンテンツデータを配布するためにCD-ROMを用いるものとして説明したが、本発明はこのような構成に限定されるものではなく、より一般的に記録媒体に記録した状態コンテンツ
10 データを配布する構成に対して適用できる。とくに限定されないが、このような記録媒体としては、他のディスク状の記録媒体、たとえば、DVD-ROM (Digital Versatile Disc Read Only Memory) 等を用いることも可能である。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となつてはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定され
15 ることが明らかに理解されるであろう。

請求の範囲

1. 暗号化コンテンツデータを複数のユーザの各端末に配布するためのデータ配信システムであって、

- 5 前記暗号化コンテンツデータと、前記暗号化コンテンツデータの復号処理に使用する復号情報データを取得するための平文付加情報データとを記録した記録媒体（200）と、

前記復号情報データを情報伝達網を介して配信するための配信サーバ（30）と、

- 10 前記記録媒体から前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納し、前記平文付加情報データに基づいて特定される前記配信サーバから前記情報伝達網を介して前記復号情報データを受信して、前記暗号化コンテンツデータを前記復号情報データに応じて復号し、前記暗号化コンテンツデータを復号して得られるコンテンツデータに対応する情報を出力するためのコンテンツデータ再生装置（100, 110）とを備える、データ配信システム。
- 15

2. 前記コンテンツデータ再生装置は、

前記記録媒体から前記暗号化コンテンツデータおよび前記平文付加情報データを読み取るための読取り手段と、

- 前記読取り手段から与えられた前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納するためのメモリ（110）と、
- 20

前記情報伝達網を介して前記特定された配信サーバから前記復号情報データを受信するための受信手段（1102, 1104）と、

前記暗号化コンテンツデータを前記復号情報データに基づいて復号するための復号手段（1530）と、

- 25 前記復号手段からの出力を受けて、前記コンテンツデータに対応する情報を再生するための再生手段（1540）とを含む、請求項1記載のデータ配信システム。

3. 前記メモリは、

前記コンテンツデータ再生装置から着脱可能なメモリカード（110）である、

請求項 2 記載のデータ配信システム。

4. 前記復号情報データは、

前記暗号化コンテンツデータを復号するためのコンテンツ復号キー（Kc）と、
前記メモリカードからの前記復号情報データの読出を制限するための第 1 の制

5 限情報データ（AC1）とを含み、

前記メモリカードは、

前記第 1 の制御情報データに応じて、前記メモリカードからの前記復号情報データの読出を制限する手段（1500, 1420）を含む、請求項 3 記載のデータ配信システム。

10 5. 前記第 1 の制御情報データは、

前記暗号化コンテンツデータを復号するために前記メモリカードからの前記コンテンツ復号キーの読出可能回数を指定するための制御データを含み、

前記メモリカードは、

15 前記制御データに応じて、前記メモリカードからの前記コンテンツ復号キーの読出回数を制限する手段を含む、請求項 4 記載のデータ配信システム。

6. 前記復号情報データは、

前記暗号化コンテンツデータを復号するためのコンテンツ復号キーと、

前記コンテンツデータ再生装置での再生条件を指定するための第 2 の制限情報データ（AC2）とを含み、

20 前記コンテンツデータ再生装置は、

前記第 2 の制御情報データに応じて、前記再生手段の再生動作を制限する手段をさらに含む、請求項 2 項に記載のデータ配信システム。

7. 前記配信サーバは、

25 前記コンテンツ復号キーと前記第 2 の制御情報データとを所定の鍵で暗号化するための第 1 の暗号化手段を備え、

前記コンテンツデータ再生装置は、

前記所定の鍵で暗号化されたデータを復号するための第 1 の復号手段を含む、請求項 6 記載のデータ配信システム。

8. 前記配信サーバ（30）は、

前記情報伝達網を介して外部との間でデータを授受するための第1のインターフェース部(350)と、

前記コンテンツ復号キーの通信ごとに更新される第1の共通鍵を生成する第1のセッションキー発生部(320)と、

- 5 前記ユーザのコンテンツデータ再生装置に対応して予め定められた第1の公開暗号鍵により前記第1の共通鍵を暗号化して前記第1のインターフェース部に与えるためのセッションキー暗号化部(322)と、

前記第1の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部(324)と、

- 10 前記復号情報データ、前記セッションキー復号部により復号されたデータから抽出される第2の公開暗号鍵により暗号化するための第1の復号情報データ暗号処理部(326)と、

- 前記第1の復号情報データ暗号処理部の出力を前記セッションキー復号部により復号されたデータから抽出される第2の共通鍵により暗号化して前記第1のインターフェース部に与え配信するための第2の復号情報データ暗号処理部(328)とを備え、
- 15

前記コンテンツデータ再生装置は、

前記情報伝達網を介して外部との間でデータを授受するための第2のインターフェース部(1102, 1104)をさらに含み、

- 20 前記メモ리카ード(110)は、

前記第2の共通鍵を生成する第2のセッションキー発生部(1312)と、

前記第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部(1304)と、

- 前記第1の公開暗号鍵によって暗号化された前記第1の共通鍵を受けて、復号処理するための第1の復号処理部(1306)と、
- 25

前記第2の公開暗号鍵を保持するための第2の鍵保持部(1310)と、

前記第2の公開暗号鍵および前記第2の共通鍵を、前記第1の共通鍵に基づいて暗号化し、前記第2のインターフェース部に出力するための第1の暗号化処理部(1340)と、

前記第 2 の復号情報データ暗号処理部からの暗号化された前記復号情報データを受け、前記第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部（1 3 5 6）と、

前記第 2 の復号処理部の復号結果を格納するための記憶部（1 4 1 0, 1 5 0 5 0）と、

前記第 2 の公開暗号鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部（1 4 1 4）と、

前記第 2 の秘密復号鍵により前記復号情報データに対する復号処理をするための第 3 の復号処理部（1 4 1 6）とを備える、請求項 3 記載のデータ配信システム。

9. 前記配信サーバは、

前記情報伝達網を介して外部との間でデータを授受するための第 1 のインターフェース部と、

前記コンテンツ復号キーの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザのコンテンツデータ再生装置に対応して予め定められた第 1 の公開暗号鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェース部に与えるためのセッションキー暗号化部と、

前記第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記復号情報データ、前記セッションキー復号部により復号されたデータから抽出される第 2 の公開暗号鍵により暗号化するための第 1 の復号情報データ暗号処理部と、

前記第 1 の復号情報データ暗号処理部の出力を前記セッションキー復号部により復号されたデータから抽出される第 2 の共通鍵により暗号化して前記第 1 のインターフェース部に与え配信するための第 2 の復号情報データ暗号処理部とを備え、

前記コンテンツデータ再生装置は、

前記情報伝達網を介して外部との間でデータを授受するための第 2 のインター

フェース部をさらに含み、

前記メモリカードは、

前記第2の共通鍵を生成する第2のセッションキー発生部と、

5 前記第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の
秘密復号鍵を保持する第1の鍵保持部と、

前記第1の公開暗号鍵によって暗号化された前記第1の共通鍵を受けて、復号
処理するための第1の復号処理部と、

前記第2の公開暗号鍵を保持するための第2の鍵保持部と、

10 前記第2の公開暗号鍵および前記第2の共通鍵を、前記第1の共通鍵に基づい
て暗号化し、前記第2のインターフェース部に出力するための第1の暗号化処理
部と、

前記第2の復号情報データ暗号処理部からの暗号化された前記復号情報データ
を受け、前記第2の共通鍵に基づいて復号化するための第2の復号処理部と、

15 前記第2の公開暗号鍵によって暗号化されたデータを復号するための第2の秘
密復号鍵を保持する第3の鍵保持部と、

前記第2の復号処理部の出力を受けて、前記第2の秘密復号鍵により前記復号
情報データに対する復号処理をするための第3の復号処理部と、

前記第3の復号処理部の出力を受けて、格納するための記憶部とを備える、請
求項3記載のデータ配信システム。

20 10. 前記情報伝達網は、デジタル携帯電話網であって、

前記コンテンツデータ再生装置は、携帯電話機(100)を含み、

前記携帯電話機は、

外部との間でデジタルデータの授受が可能なデータ入出力端子(1120)と、

25 前記携帯電話機に着脱可能であって、前記記録媒体から読み出され前記データ
入出力端子を介して与えられた前記暗号化コンテンツデータおよび前記平文付加
情報データを受けて格納するためのメモリカード(110)と、

前記デジタル携帯電話網を介して前記特定された配信サーバから受信した前記
復号情報データに基づいて、前記暗号化コンテンツデータを復号するための復号
手段(1530)と、

前記復号手段からの出力を受けて、前記コンテンツデータに対応する情報を再生するための再生手段（１５４０）とを含む、請求項１記載のデータ配信システム。

１１．前記復号情報データは、

５ 前記暗号化コンテンツデータを復号するためのコンテンツ復号キーと、

前記メモリカードからの前記復号情報データの読出を制限するための第１の制限情報データとを含み、

前記メモリカードは、

前記第１の制御情報データに応じて、前記メモリカードからの前記復号情報データの読出を制限する手段を含む、請求項１０に記載のデータ配信システム。

１２．前記第１の制御情報データは、

前記暗号化コンテンツデータを復号するために前記メモリカードからのコンテンツ復号キーの読出可能回数を指定するための制御データを含み、

前記メモリカードは、

１５ 前記制御データに応じて、前記メモリカードからの前記コンテンツ復号キーの読出回数を制限する手段を含む、請求項１０記載のデータ配信システム。

１３．前記復号情報データは、

前記暗号化コンテンツデータを復号するためのコンテンツ復号キーと、

前記コンテンツデータ再生装置での再生条件を指定するための第２の制限情報データとを含み、

前記コンテンツデータ再生装置は、

前記第２の制御情報データに応じて、前記再生手段の再生動作を制限する手段をさらに含む、請求項１０に記載のデータ配信システム。

１４．前記配信サーバは、

２５ 前記コンテンツ復号キーと前記第２の制御情報データとを所定の鍵で暗号化するための第１の暗号化手段を備え、

前記コンテンツデータ再生装置は、

前記所定の鍵で暗号化されたデータを復号するための第１の復号手段を含む、請求項１３記載のデータ配信システム。

15. 前記携帯電話機は、前記コンテンツデータ再生装置から着脱可能である、請求項10記載のデータ配信システム。

16. 前記情報伝達網は、デジタル携帯電話網であって、
前記コンテンツデータ再生装置は、

5 前記デジタル携帯電話網を介して前記特定された配信サーバから前記復号情報データを受信するための携帯電話機を含み、

前記携帯電話機は、

前記暗号化コンテンツデータを前記復号情報データに基づいて復号するための復号手段と、

10 前記復号手段からの出力を受けて、前記コンテンツデータに対応する情報を再生する再生手段とを有し、

前記コンテンツデータ再生装置は、

前記携帯電話機に着脱可能であって、前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納するためのメモ리카ードと、

15 前記記録媒体から前記メモ리카ードへのデータ転送を行うためのメモ리카ードドライブ装置とをさらに含む、請求項1記載のデータ配信システム。

17. 前記復号情報データは、

前記暗号化コンテンツデータを復号するためのコンテンツ復号キーと、

前記メモ리카ードからの前記復号情報データの読出を制限するための第1の制限情報データとを含み、

20 前記メモ리카ードは、

前記第1の制御情報データに応じて、前記メモ리카ードからの前記復号情報データの読出を制限する手段を含む、請求項16に記載のデータ配信システム。

18. 前記第1の制御情報データは、

25 前記暗号化コンテンツデータを復号するために前記メモ리카ードからのコンテンツ復号キーの読出可能回数を指定するための制御データを含み、

前記メモ리카ードは、

前記制御データに応じて、前記メモ리카ードからの前記コンテンツ復号キーの読出回数を制限する手段を含む、請求項17記載のデータ配信システム。

19. 前記復号情報データは、

前記暗号化コンテンツデータを復号するためのコンテンツ復号キーと、

前記コンテンツデータ再生装置での再生条件を指定するための第2の制限情報データとを含み、

5 前記コンテンツデータ再生装置は、

前記第2の制御情報データに応じて、前記再生手段の再生動作を制限する手段をさらに含む、請求項16記載のデータ配信システム。

20. 前記配信サーバは、

10 前記コンテンツ復号キーと前記第2の制御情報データとを所定の鍵で暗号化するための第1の暗号化手段を備え、

前記コンテンツデータ再生装置は、

前記所定の鍵で暗号化されたデータを復号するための第1の復号手段を含む、請求項19記載のデータ配信システム。

21. 前記情報伝達網は、デジタル携帯電話網であって、

15 前記コンテンツデータ再生装置は、

前記デジタル携帯電話網を介して前記特定された配信サーバから前記復号情報データを受信するための携帯電話機を含み、

前記携帯電話機は、

20 前記暗号化コンテンツデータを前記復号情報データに基づいて復号するための復号手段と、

前記復号手段からの出力を受けて、前記コンテンツデータに対応する情報を再生する再生手段とを有し、

前記コンテンツデータ再生装置は、

25 前記携帯電話機に着脱可能であって、前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納するためのメモ리카ードと、

前記記録媒体から前記メモ리카ードへのデータ転送を行うためのメモ리카ードドライブ装置(500)をさらに含む、

前記記録媒体は、暗号化コンテンツデータ、平文付加情報、予め定められた複数の固有鍵を特定するための特定データおよび特定データに対応する固有鍵によ

り復号可能な暗号化をされた復号情報データを記録しており、

前記メモ리카ードドライブ装置は、

前記特定データにより選択的に指定される複数の固有鍵を保持する固有鍵保持部と、

- 5 前記複数の固有鍵のうち、前記記録媒体からの前記特定データに対応する固有鍵で、前記記録媒体からの前記暗号化された復号情報データを復号して、復号情報データを受理する固有鍵復号処理部とを有し、

- 10 少なくとも前記メモ리카ードドライブ装置において前記復号情報データを受理可能であることに基づいて、前記メモ리카ードへ前記受理した復号情報データが転送される、請求項 1 記載のデータ配信システム。

2 2. 暗号化コンテンツデータを複数のユーザの各端末に配布するためのデータ配信システムであって、

- 15 前記暗号化コンテンツデータと、前記暗号化コンテンツデータの復号処理に使用する復号情報データを取得するための平文付加情報データとを記録した記録媒体と、

- 20 前記記録媒体から前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納し、前記平文付加情報データに基づいて特定される前記配信サーバから情報伝達網を介して前記復号情報データを受信して、前記暗号化コンテンツデータを前記復号情報データに応じて復号し、前記暗号化コンテンツデータを復号して得られるコンテンツデータに対応する情報を出力するためのコンテンツデータ再生装置とを備える、データ配信システム。

2 3. 前記コンテンツデータ再生装置は、

前記記録媒体から前記暗号化コンテンツデータおよび前記平文付加情報データを読み取るための読取り手段と、

- 25 前記読取り手段から与えられた前記暗号化コンテンツデータおよび前記平文付加情報データを受けて格納するためのメモリと、

前記情報伝達網を介して前記特定された配信サーバから前記復号情報データを受信するための受信手段と、

前記暗号化コンテンツデータを前記復号情報データに基づいて復号するための

復号手段と、

前記復号手段からの出力を受けて、前記コンテンツデータに対応する情報を再生するための再生手段とを含む、請求項 22 記載のデータ配信システム。

24. 前記メモリは、

- 5 前記コンテンツデータ再生装置から着脱可能なメモリカードである、請求項 23 記載のデータ配信システム。

25. 暗号化コンテンツデータを複数のユーザの各端末に配布するために、前記暗号化コンテンツデータの復号処理に使用する復号情報データを情報伝達網を介して配信するための配信サーバを備え、各前記端末は、前記暗号化コンテンツデータおよび平文付加情報データを受けて格納し、前記平文付加情報に基づいて特定される前記配信サーバから前記情報伝達網を介して前記復号情報データを受信して、前記暗号化コンテンツデータを前記復号情報データに応じて復号し、前記暗号化コンテンツデータを復号して得られるコンテンツデータに対応する情報を出力するためのコンテンツデータ再生装置とを備えるデータ配信システムに用い
10 られる記録媒体であって、

少なくとも前記暗号化コンテンツデータを記録するための第 1 の領域と、

前記暗号化コンテンツデータの復号処理に使用する前記復号情報データを取得するための前記平文付加情報データとを記録するための第 2 の領域とを備える、
記録媒体。

- 20 26. 前記記録媒体は、

暗号化された前記復号情報データを記録するための第 3 の領域をさらに備え、

前記復号情報データは、前記暗号化コンテンツデータの再生を制限するための制御情報データを含む、請求項 25 記載の記録媒体。

27. 前記記録媒体は、ディスク状記録媒体である、請求項 25 記載の記録媒体。

- 25 28. 前記記録媒体は、CD-ROM である、請求項 25 記載の記録媒体。

29. 前記記録媒体は、DVD-ROM である、請求項 25 記載の記録媒体。

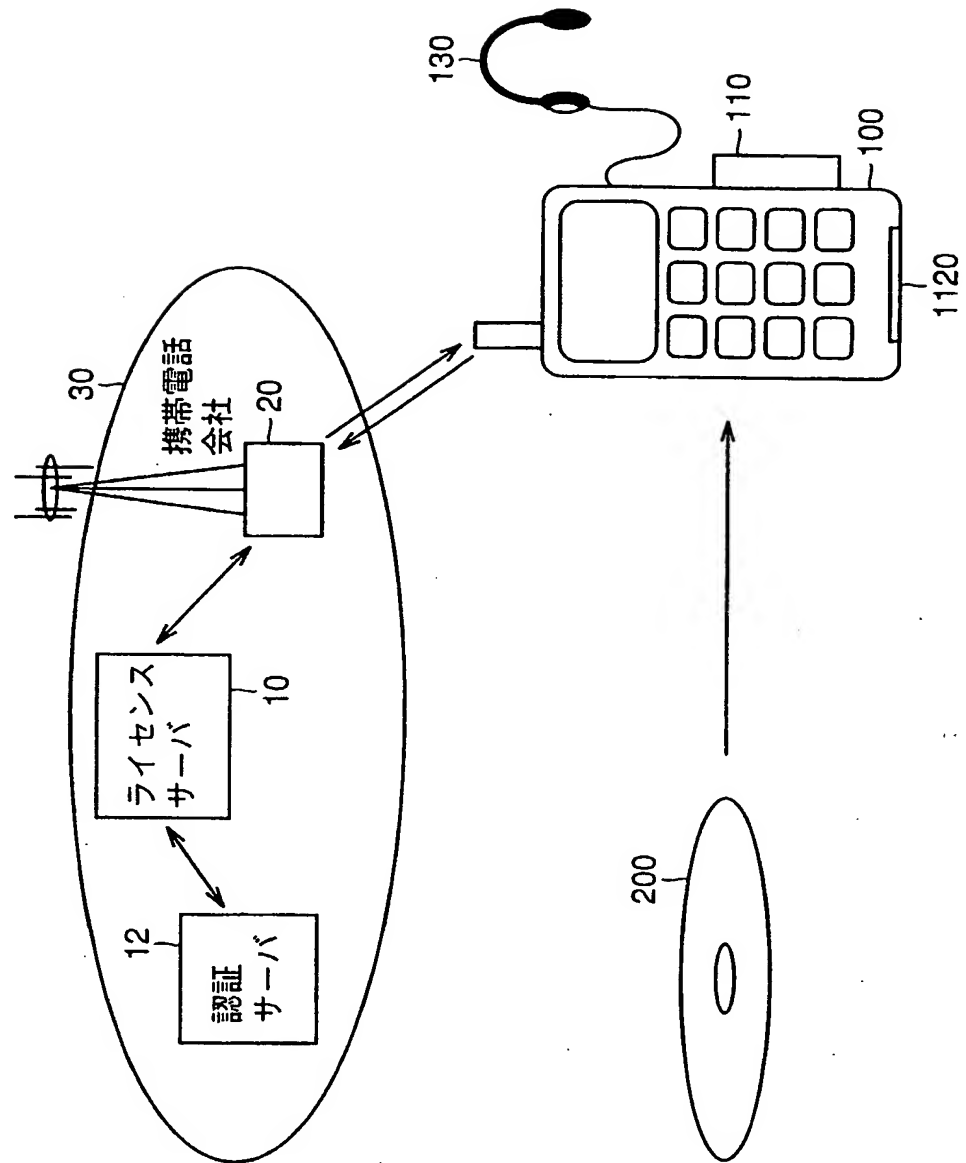


FIG. 1

FIG.2

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて、CD-ROMにて配布 例) 音楽データ、映像データ	CD-ROM
Data-inf	付加情報データ、コンテンツデータに関する著作権関連あるいはサーバアクセス関連等の平文情報	CD-ROM
Kc	コンテンツ復号キー	配信サーバ
Kp	コンテンツ再生部固有の復号鍵	携帯電話機
KPp	Kpにて復号可能な暗号化鍵、公開復号鍵KPmaにて復号することで認証機能を有する{KPp}KPmaの形式でメモリ内に記録	携帯電話機
Kcom	データ再生装置(携帯電話機)に共通の復号鍵、Kc、AC2の授受に利用	配信サーバ 携帯電話機
AC1	メモリのアクセスに対する制御情報(例えば再生回数の制限)	配信サーバ
AC2	データ再生装置に対する制限する制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵	メモリカード
KPm(i)	Km(i)にて復号可能な暗号化鍵	メモリカード
Kmc	メディア(メモリカードの種類など)依存の復号鍵	メモリカード
KPmc	Kmcにて復号可能な暗号化鍵、公開復号鍵KPmaにて復号することで認証機能を有する{KPmc}KPmaの形式でメモリカード内に記録	メモリカード
KPma	システム共通の復号鍵(公開)	配信サーバ
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	CD-ROM
ライセンスID	ライセンスの配信を特定できる管理コード(コンテンツIDをも含めて識別することもある)	配信サーバ

FIG.3

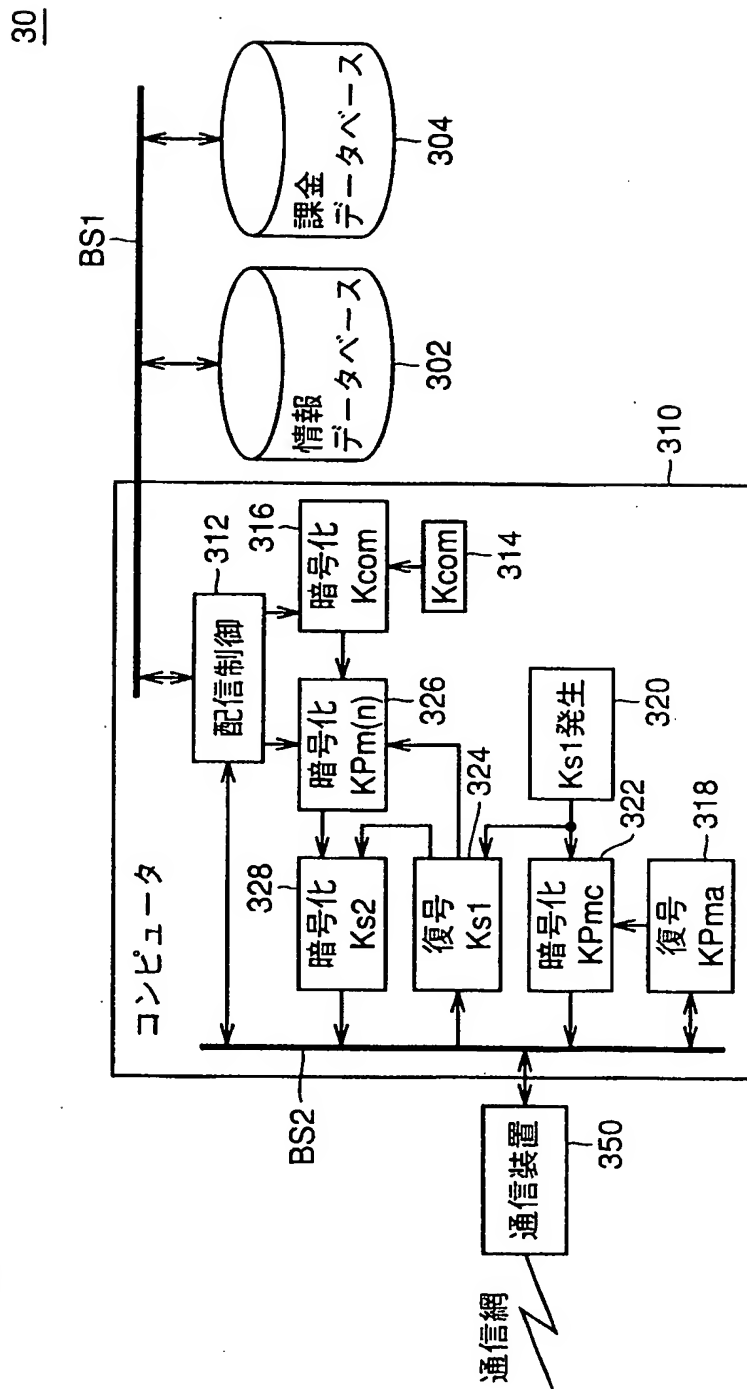


FIG. 4

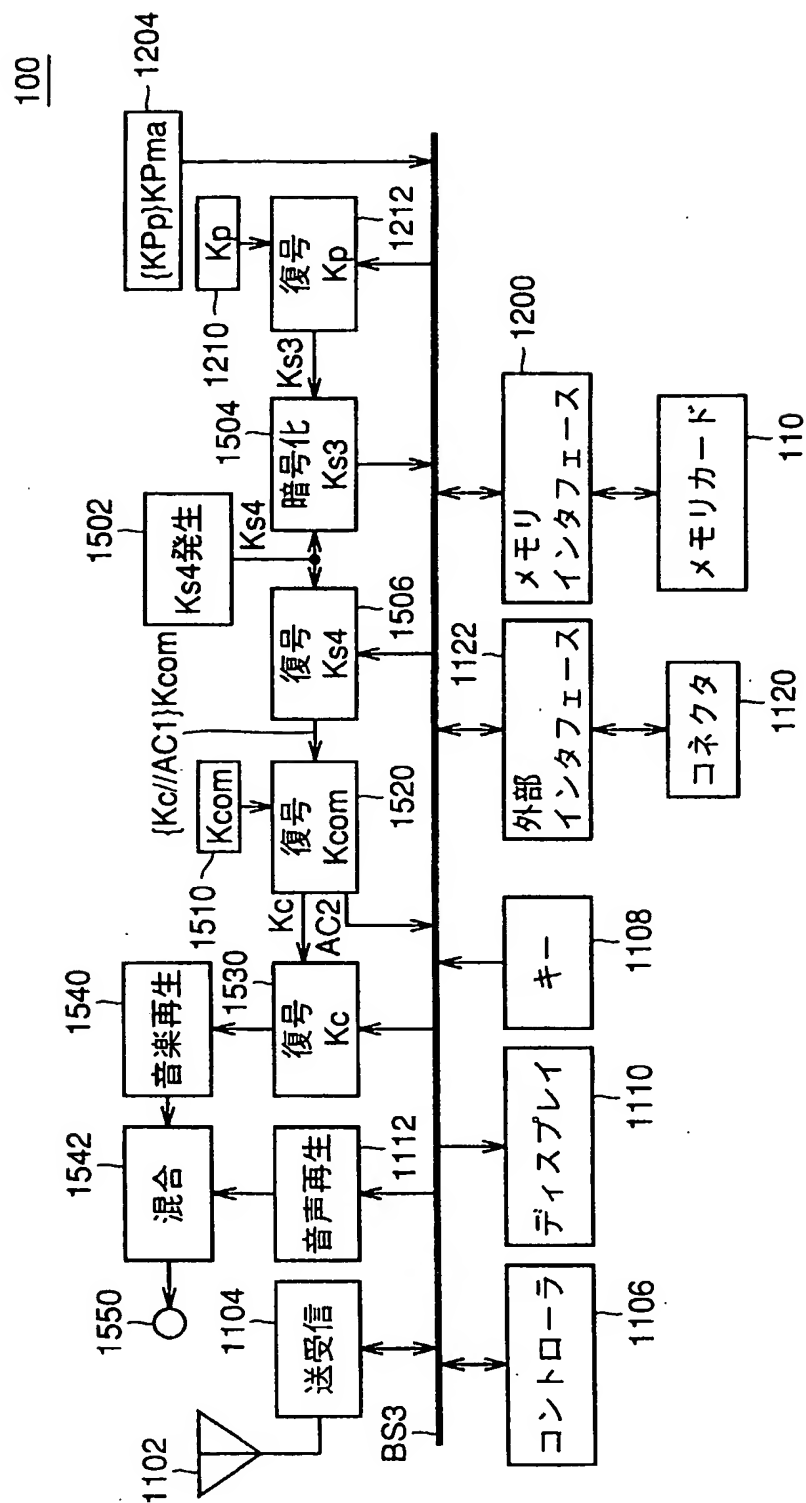


FIG.5

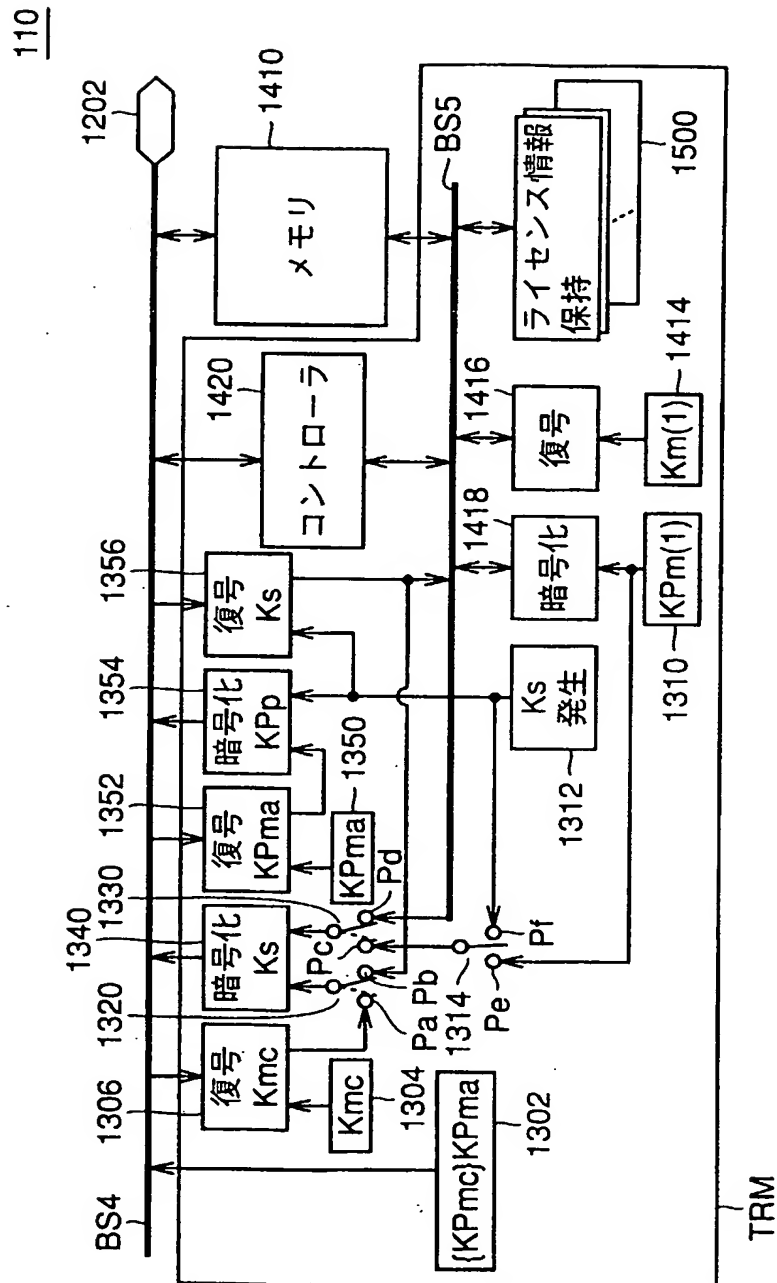


FIG.6

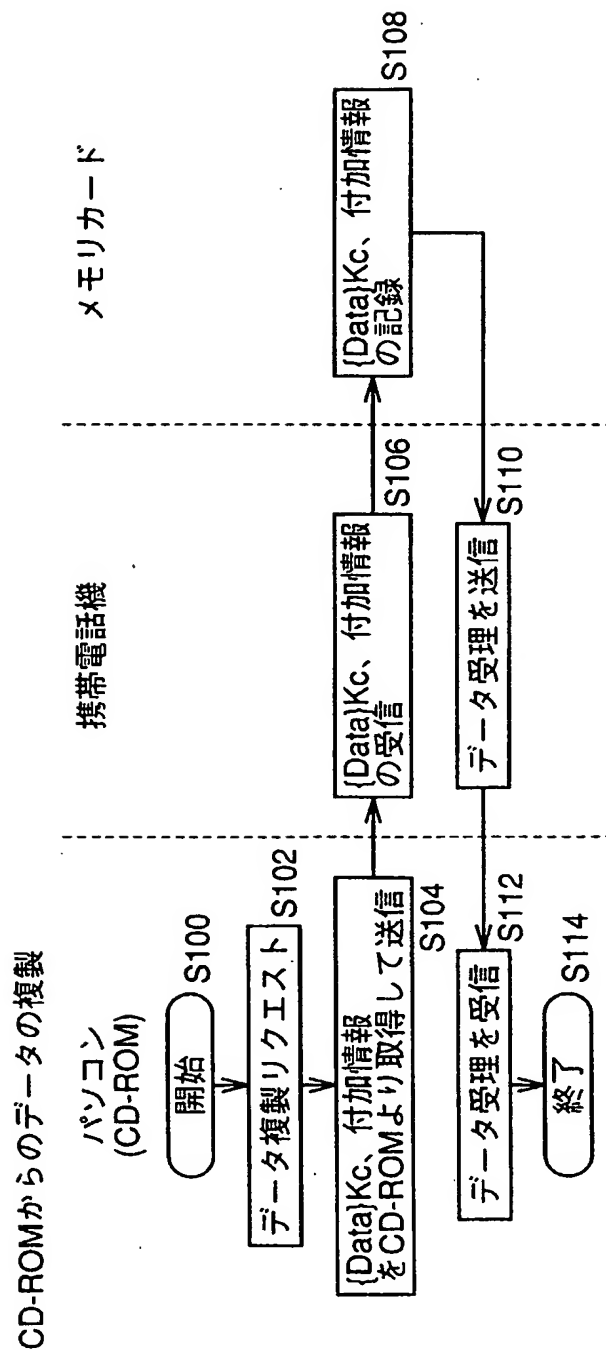


FIG. 7

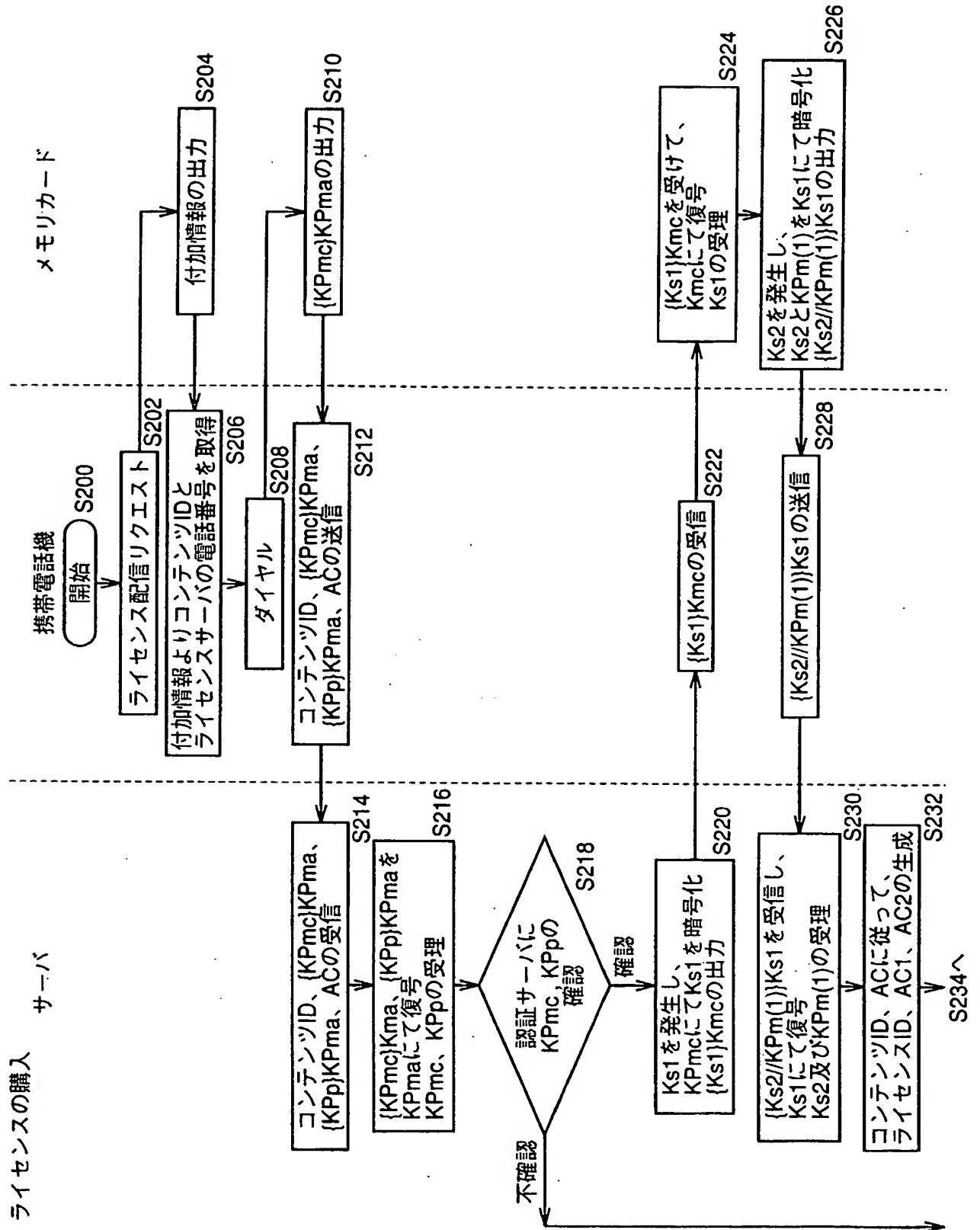


FIG.8

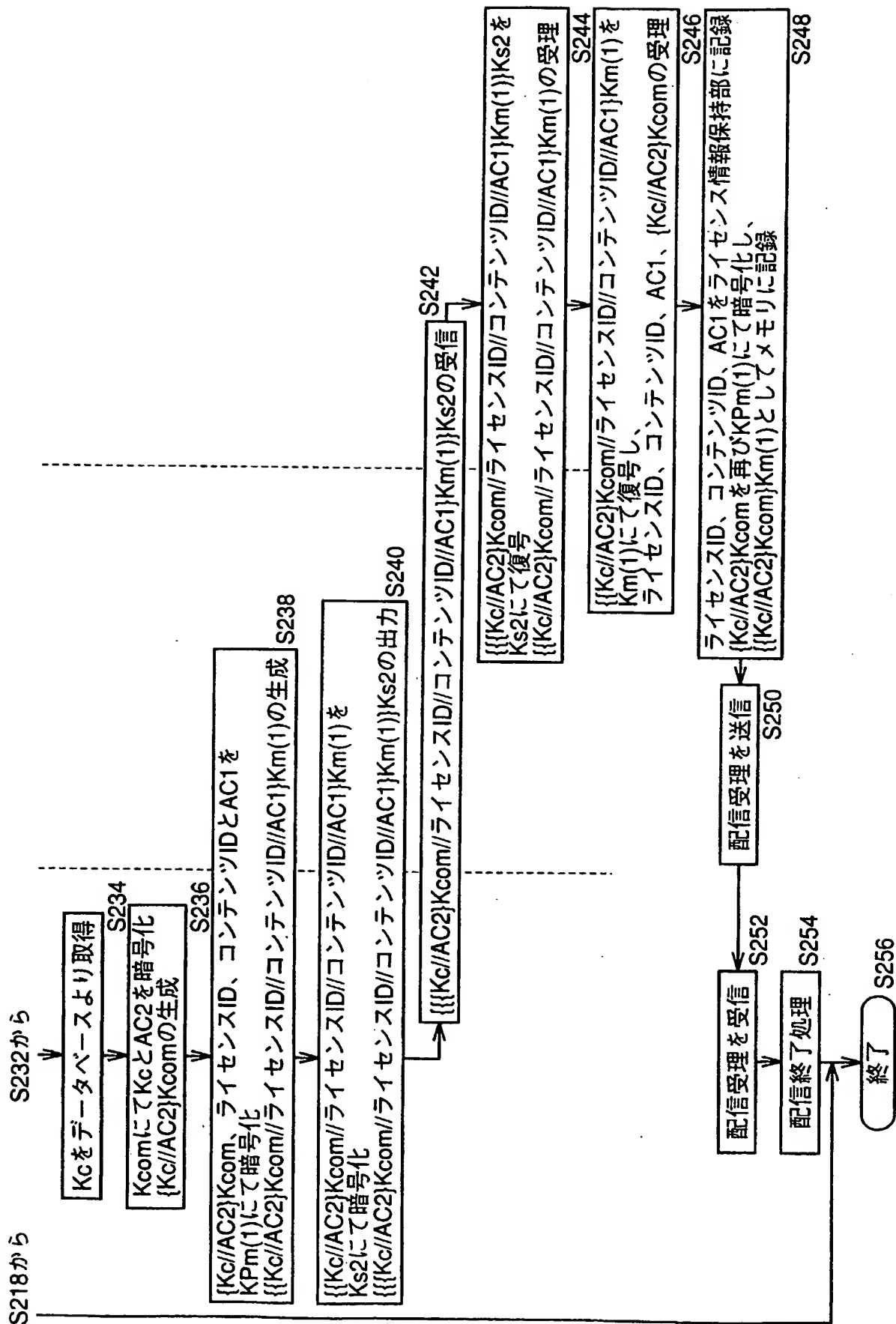


FIG.9

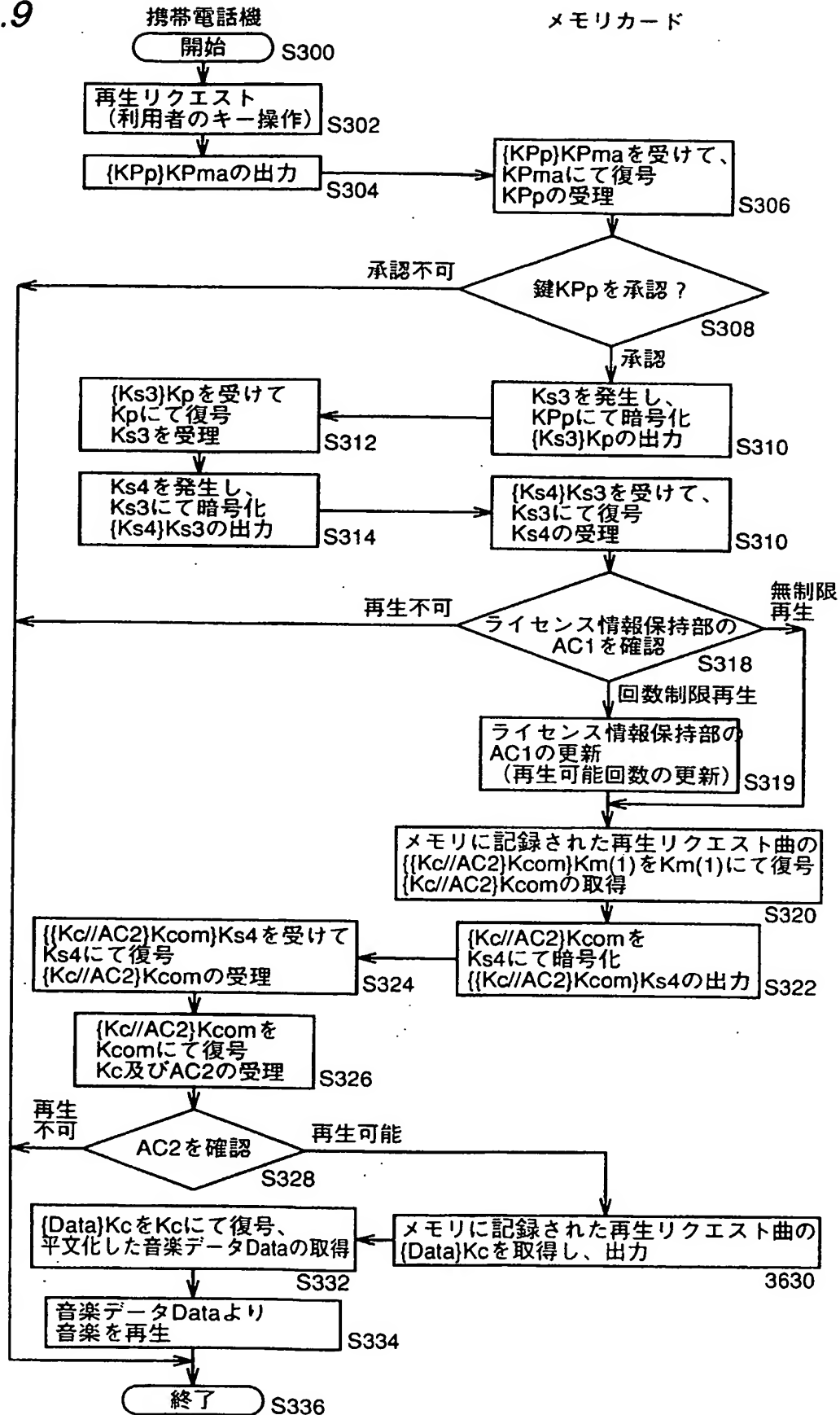
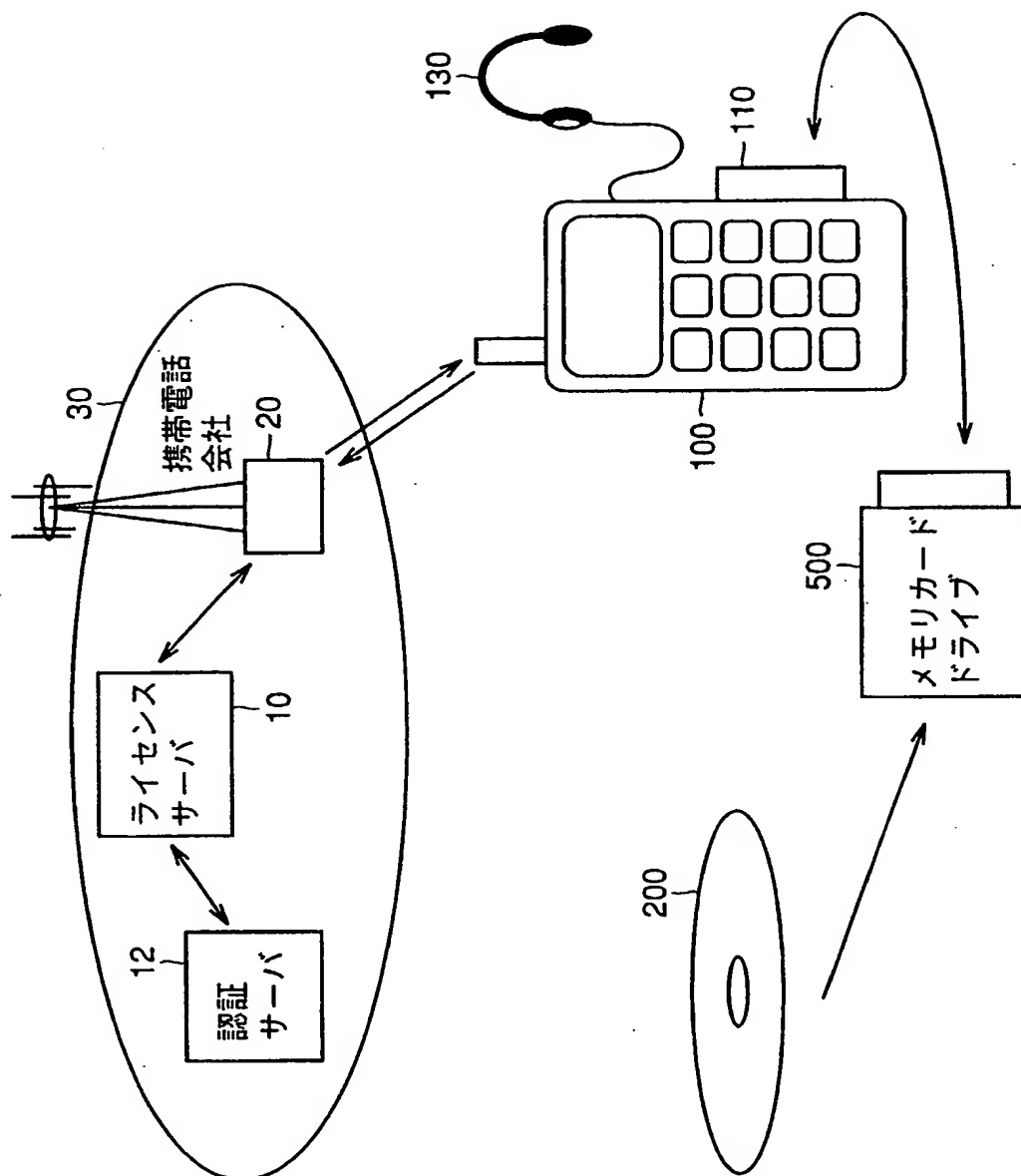


FIG.10



500

FIG. 11

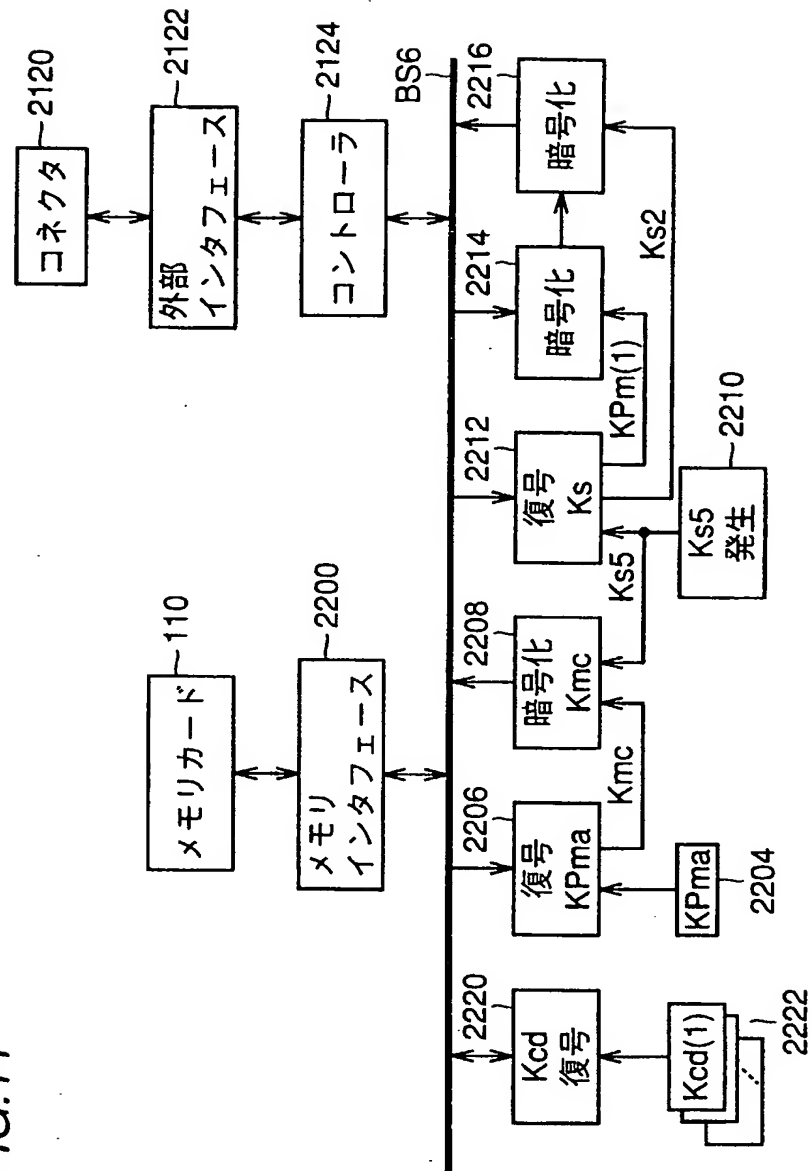


FIG. 12

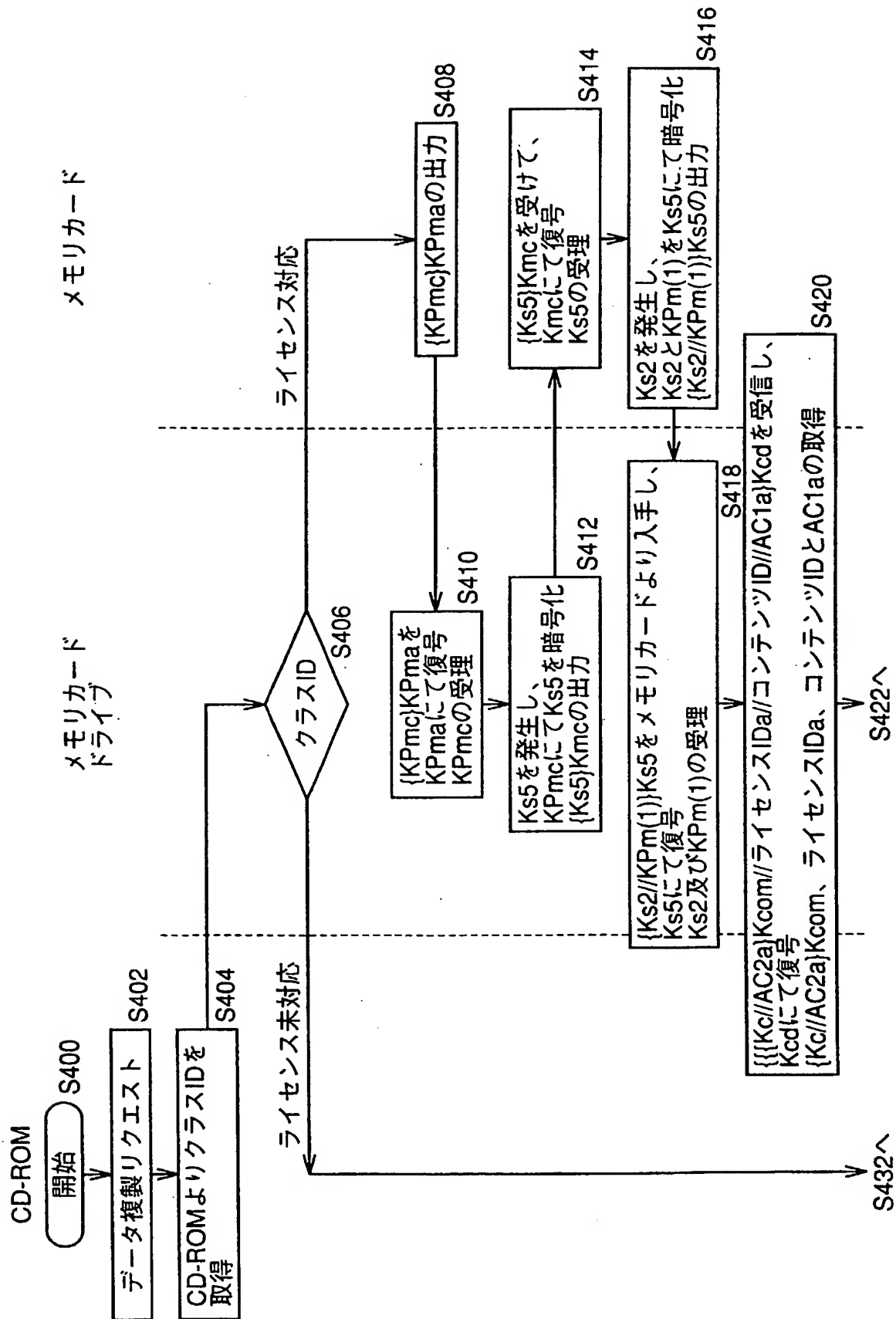


FIG. 13

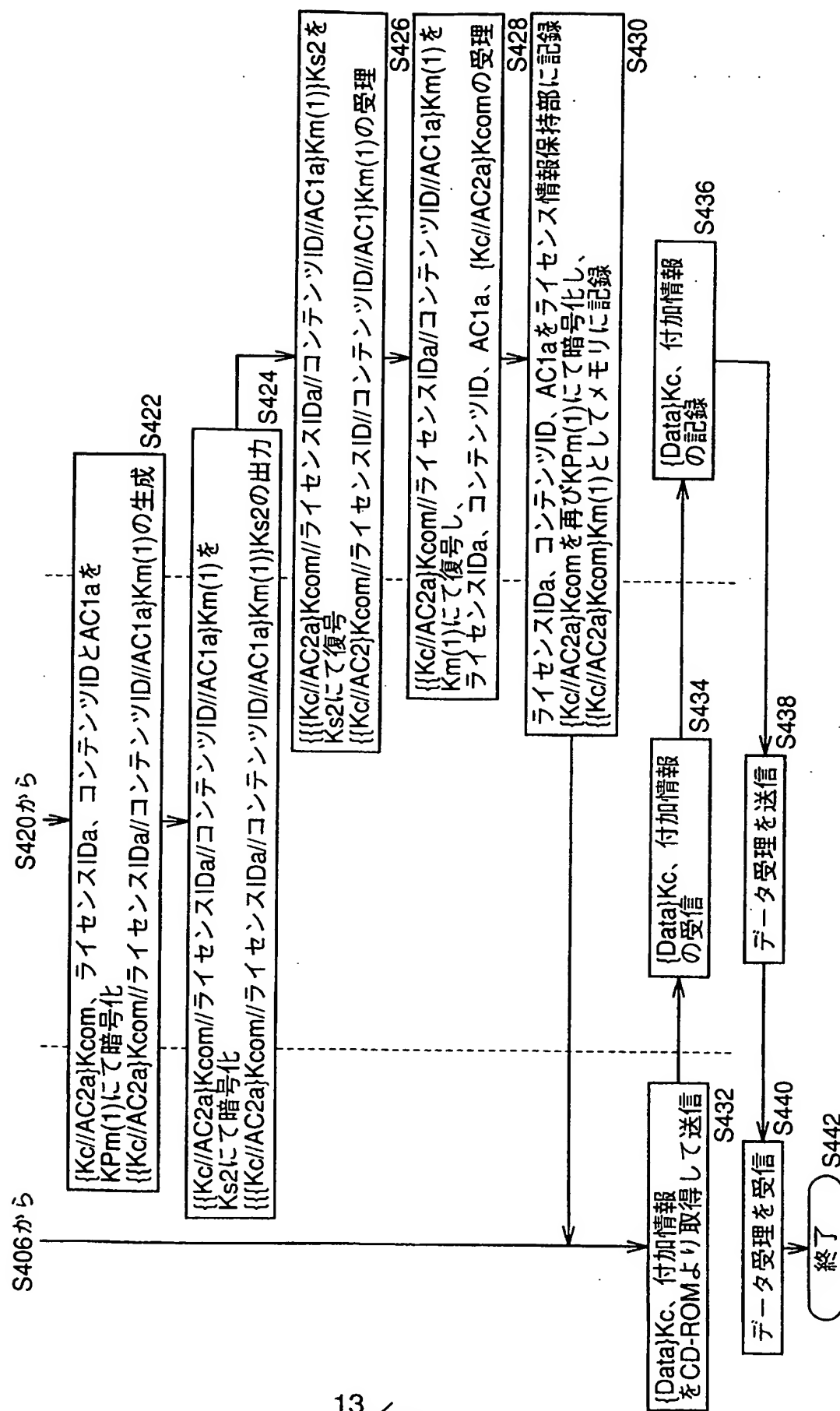


FIG. 14

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて、CD-ROMにて配布 例) 音楽データ、映像データ	CD-ROM
Data-inf	付加情報データ、コンテンツデータに関する著作権関連あるいはサーバアクセス関連等の平文情報	CD-ROM
Kc	コンテンツ復号キー	配信サーバ
Kp	コンテンツ再生部固有の復号鍵	携帯電話機
KPp	Kpにて復号可能な暗号化鍵、公開復号鍵KPmaにて復号することで認証機能を有する{KPp}KPmaの形式でメモリ内に記録	携帯電話機
AC1	メモリのアクセスに対する制御情報(例えば再生回数の制限)	配信サーバ
AC2	データ再生装置に対する制限する制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵	メモリカード
KPm(i)	Km(i)にて復号可能な暗号化鍵	メモリカード
Kmc	メディア(メモリカードの種類など)依存の復号鍵	メモリカード
KPmc	Kmcにて復号可能な暗号化鍵、公開復号鍵KPmaにて復号することで認証機能を有する{KPmc}KPmaの形式でメモリカード内に記録	メモリカード
KPma	システム共通の復号鍵(公開)	配信サーバ
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	CD-ROM
ライセンスID	ライセンスの配信を特定できる管理コード(コンテンツIDをも含めて識別することもある)	配信サーバ

FIG. 15

31

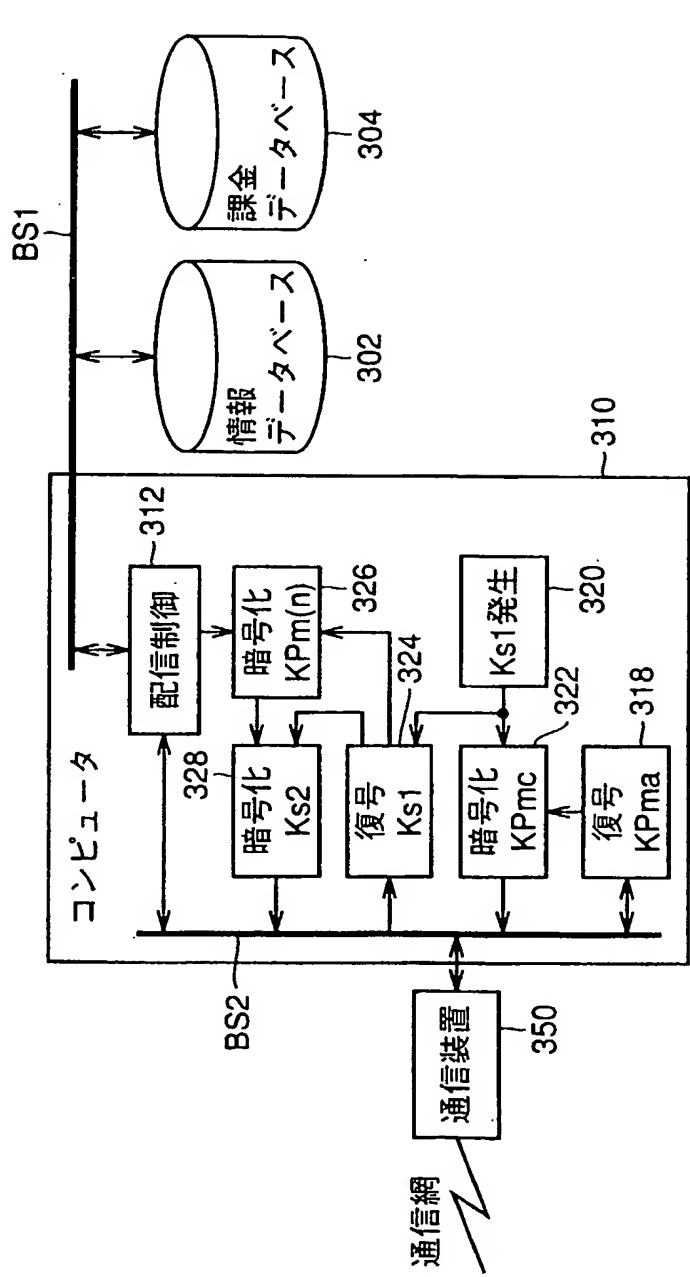


FIG. 16

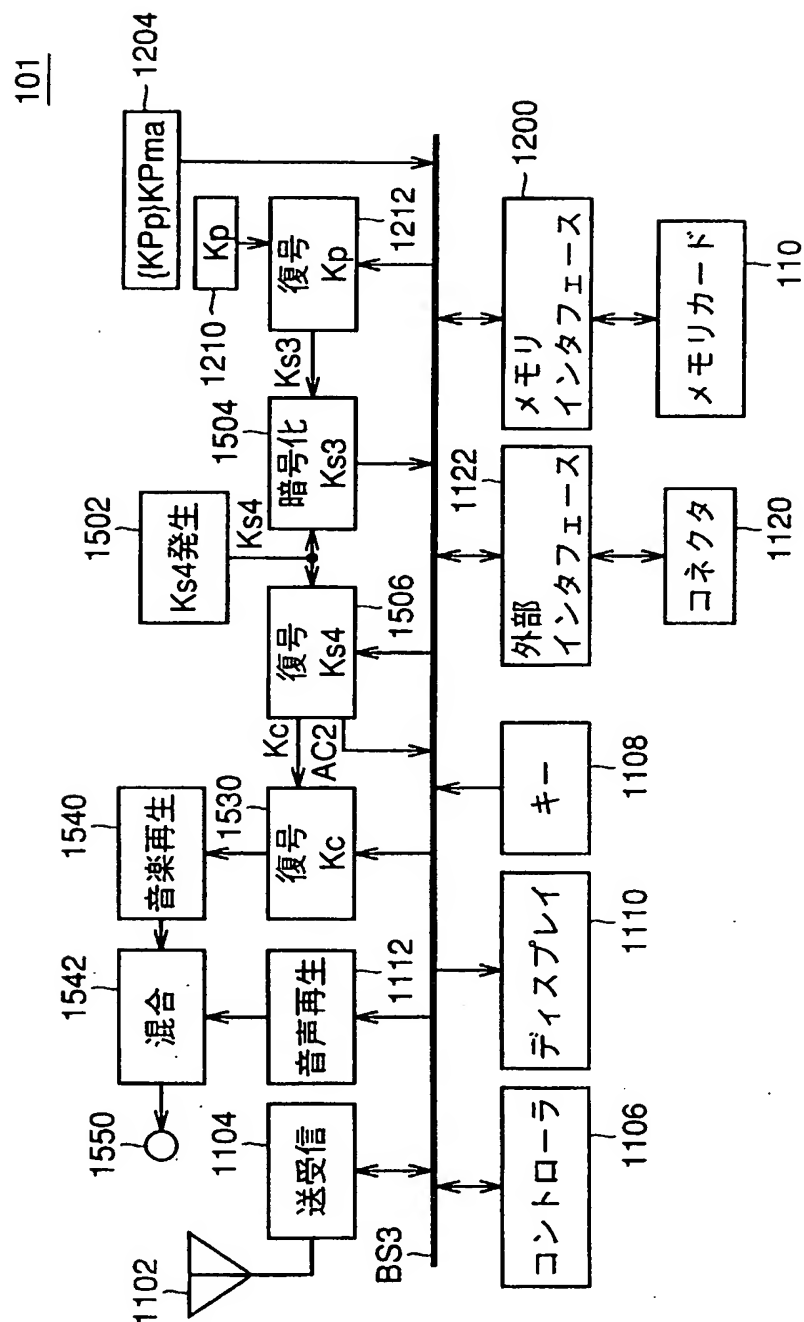


FIG.17

ライセンスの購入

サーバ

携帯電話機

メモリカード

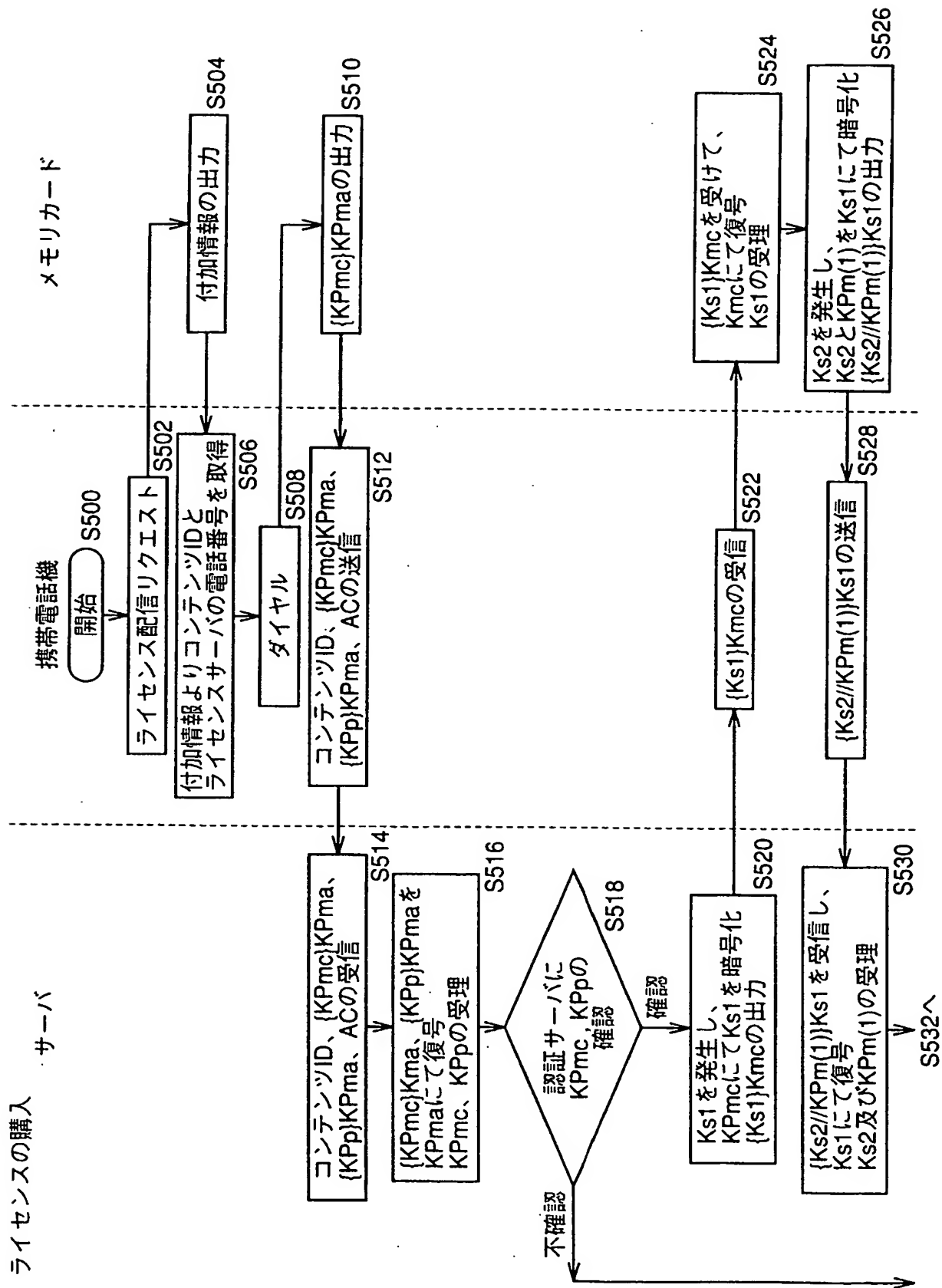


FIG. 18

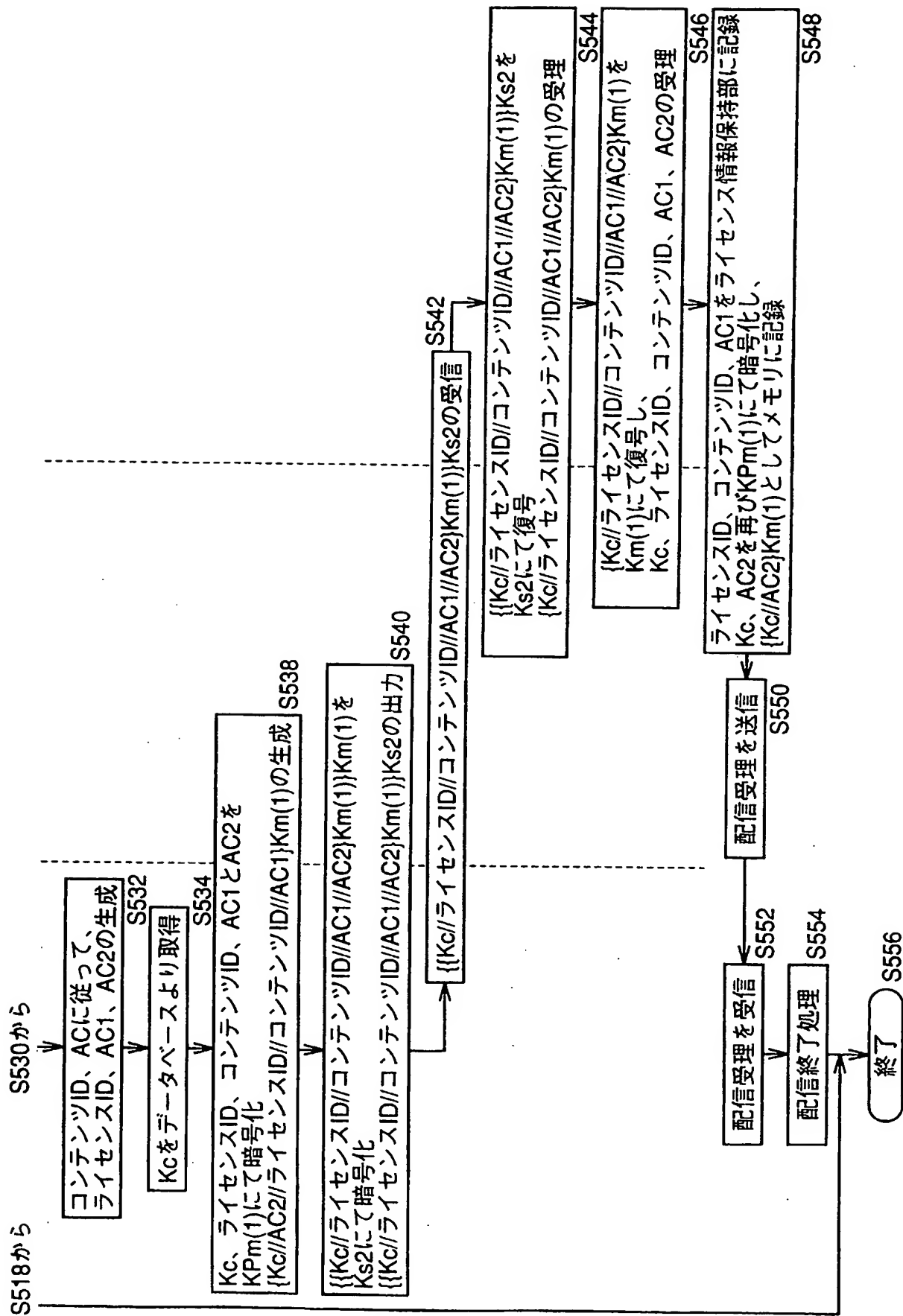
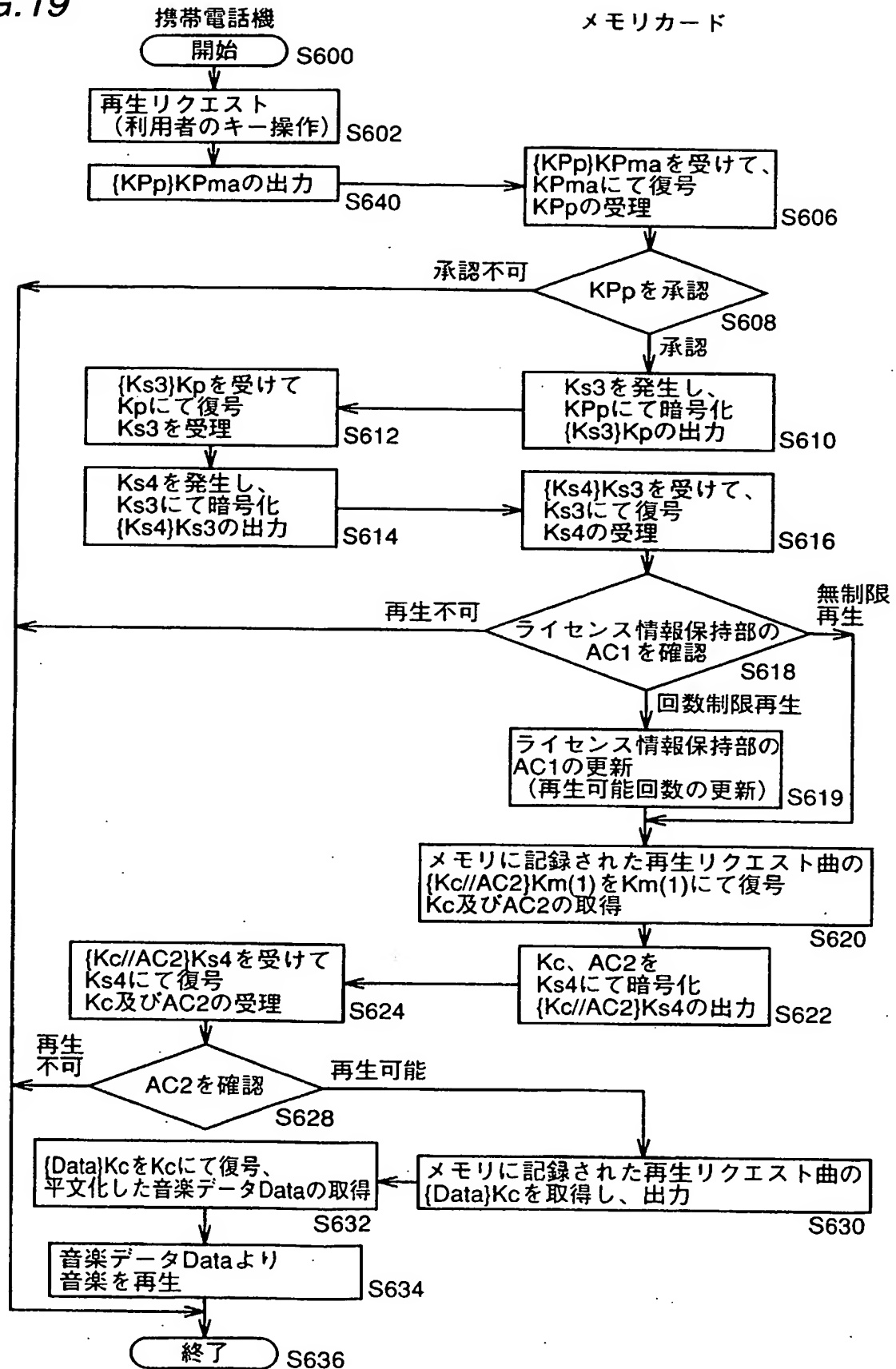


FIG. 19



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08107

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.⁷ H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl.⁷ H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Kiyoshi YAMANAKA, et al., "Multimedia on Demand System Service ni okeru Joho Hogo System", NTT R&D, Vol.44, No.9, (1995), pp.813-818 Especially, Fig.3	1-3, 22-25 27-29
Y	Full text; Figs. 1-4	4-21, 26
Y	JP, 10-40172, A (Toshiba Corporation), 13 February, 1998 (13.02.98), Full text; Figs. 1 to 4 (Family: none)	4-21, 26
X	JP, 9-34841, A (Fujitsu Limited), 07 February, 1997 (07.02.97), especially, Figs. 2, 3	1-3, 22-25 27-29
A	Full text; Figs. 1-27 (Family: none)	4-21, 26
A	JP, 11-265317, A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 September, 1999 (28.09.99), Full text; Figs. 1 to 4 (Family: none)	1-29
A	JP, 9-307543, A (Matsushita Electric Ind. Co., Ltd.),	1-29

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 28 February, 2001 (28.02.01)	Date of mailing of the international search report 13 March, 2001 (13.03.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08107

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	28 November, 1997 (28.11.97), Full text; Figs. 1 to 8 (Family: none)	
A	JP, 11-154944, A (NTT DATA CORPORATION), 08 June, 1999 (08.06.99), Full text; Figs. 1 to 9 (Family: none)	1-29
A	JP, 11-164058, A (Hitachi Electron Service Co., Ltd.), 18 June, 1999 (18.06.99), Full text; Figs. 1 to 2 (Family: none)	1-29
A	Seigo KOTANI, et al., "Secure PC Card" FUJITSU, Vol.49, No.3, (1998), pp.246-249	1-29

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	山中 喜義, 高嶋 洋一, 小柳津 育郎 “マルチメディアオンデマンドシステムサービスにおける情報保護システム” NTT R&D, Vol. 44, No. 9, (1995), pp. 813-818 特に第3図参照	1-3, 22-25 27-29
Y	全文, 第1-4図	4-21, 26
Y	JP, 10-40172, A (株式会社東芝) 13. 2月. 1998 (13. 02. 98) 全文, 第1-4図 (ファミリーなし)	4-21, 26

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

28. 02. 01

国際調査報告の発送日

13.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳



5W

2956

電話番号 03-3581-1101 内線 3535

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 9-34841, A (富士通株式会社) 7. 2月. 1997 (07. 02. 97) 特に第2図及び第3図参照	1-3, 22-25 27-29 4-21, 26
A	全文, 第1-27図 (ファミリーなし)	
A	J P, 11-265317, A (日本電信電話株式会社) 28. 9月. 1999 (28. 09. 99) 全文, 第1-4図 (ファミリーなし)	1-29
A	J P, 9-307543, A (松下電器産業株式会社) 28. 11月. 1997 (28. 11. 97) 全文, 第1-8図 (ファミリーなし)	1-29
A	J P, 11-154944, A (株式会社エヌ・ティ・ティ・データ) 8. 6月. 1999 (08. 06. 99) 全文, 第1-9図 (ファミリーなし)	1-29
A	J P, 11-164058, A (日立電子サービス株式会社) 18. 6月. 1999 (18. 06. 99) 全文, 第1-2図 (ファミリーなし)	1-29
A	小谷 誠剛 他 “セキュアPCカード” F U J I T S U, Vol. 49, No. 3, (1998), pp. 246-249	1-29